

Information Management

# **ARMY KNOWLEDGE MANAGEMENT AND INFORMATION TECHNOLOGY MANAGEMENT**

Headquarters  
Department of the Army  
Washington, DC  
30 June 2004

**UNCLASSIFIED**

# Chapter 8

## Records Management Policy

### **Records Management Policy, page 60**

Mission • 8–1, *page 60*

Management concept • 8–2, *page 61*

Life-cycle management of records • 8–3, *page 63*

Tenets • 8–4, *page 64*

Major subprograms • 8–5, *page 64*

General policies • 8–6, *page 66*

Record media • 8–7, *page 67*

Electronic records management • 8–8, *page 68*

### **Appendixes**

**A.** References, *page 71*

**B.** Telecommunications Services Authorized for Specific Activities, *page 80*

**C.** Management Control Evaluation Checklist, *page 83*

### **Table List**

Table 7–1: Types of VI Activities, *page 51*

### **Glossary**

---

Note: Per DA General Order 1997–24, the records management function transferred from the CIO/G–6 (formerly known as DISC4) to the DCS, G–1. Performance of the missions and functions will continue to be subject to the oversight of the CIO/G–6.

### **8–1. Mission**

The mission of records management is to capture, preserve, and make available evidence essential for Army decisions

and actions; meet the needs of the American public; and protect the rights and interests of the Government and individuals. This program will operate in accordance with public law and regulatory guidance.

## **8–2. Management concept**

*a.* Records management plans, policies, and programs provide for the modern, efficient, and systematic life-cycle management of all information of record value, regardless of format or media. It establishes requirements for agency heads and commanders at all echelons to document the Army's official business and ensure accessibility of record information throughout the lifecycle of the information; keeps the DA in compliance with information access laws; and protects the rights and interests of the Army, its soldiers, veterans and their families, and the American public. In addition, civil penalties may be imposed for violating the Freedom of Information Act (AR 25–55), and civil and criminal penalties may be imposed for violating the Privacy Act (AR 340–21).

*b.* This chapter implements the following DOD directives and instructions:

- (1) DOD 4525.8–M, Official Mail Manual.
- (2) DODD 5025.12, Standardization of Military and Associated Terminology.
- (3) DODD 5015.2, DOD Records Management Program.
- (4) DOD 5400.7–R, DOD Freedom of Information Act Program.
- (5) DODD 5025.1, DOD Directives System
- (6) DODD 5400.11, DOD Privacy Program.
- (7) DODD 8910.1, Management and Control of Information Requirements.
- (8) DOD 5015.2 STD, Design Criteria Standard for Electronic Records Management Software Applications.
- (9) DODI 5040.6, Life-Cycle Management of DOD Visual Information (VI).

*c.* Title 44, Section 3102 of the United States Code (44 USC 3102) requires the head of each Federal Agency to maintain a continuing program for the economical and efficient management of the records of the agency.

*d.* The Records Management Program includes the following provisions:

(1) Creating by the most efficient, economical, and technologically advanced methods only that information essential for conducting operations and preserving that information as records.

(2) Establishing effective controls over the creation, organization, maintenance, use, and disposition of Army record information.

(3) Providing for the most expeditious and accurate distribution of record information at a minimum cost by applying advanced technology and eliminating all but essential processing procedures.

(4) Ensuring that permanently valuable information is preserved and all other record information is retained, reviewed, and disposed of systematically as prescribed by AR 25–400–2.

(5) Establishing the management program for Army electronic recordkeeping systems.

*e.* Within the Federal Government, records are considered to be any of the following if they are made or received by any DA entity under Federal law or in connection with the transaction of public business and preserved—or are appropriate for preservation by DA as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of DA or because of the informational value of the data in them.

(1) All documents, books, papers, maps, photographs, and graphic art.

(2) Record information stored on machine-readable media. These include magnetic media (hard disks, tapes, diskettes), optical recording media (for example, laser disk, optical disk, optical card, optical tape, CD, DVD), all electronic formats (office automation software—for example, word processing, spreadsheet, presentation), e-mail, Web sites, information systems, databases, and printouts.

(3) Record information stored on film slides, aperture cards, roll microfilm, microfiche, videotape, overhead transparencies, and motion picture films.

(4) Audio and video recordings (set forth in DODI 5040.6 and chap 7).

(5) Any other documentary materials regardless of physical form or characteristics.

*f.* The following are not included within the statutory definition of the word “record” (DOD 5400.7–R, AR 25–55):

(1) Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience or reference, and stocks of publications and processed documents. Extra copies of such materials should be kept to a minimum.

(2) Objects or articles—such as structures, furniture, paintings, sculptures, three-dimensional models, vehicles, and equipment—regardless of their historical value or value as evidence.

(3) Commercially exploitable resources, including but not limited to:

(*a*) Maps, charts, map compilation manuscripts, map research materials, and data, if not created or used as primary sources of information about organizations, policies, functions, decisions, or procedures of DA.

(*b*) Computer software, if not created or used as primary sources of information about organizations, policies, functions, decisions, or procedures of DA. This does not include the underlying data processed and produced by such software, which may in some instances be stored with the software.

- (4) Unaltered publications and processed documents, such as regulations, manuals, maps, charts, and related geographical materials, that are available to the public through an established distribution system, with or without charges.
- (5) Intangible information, such as an individual's memory or oral communication.
- (6) Personal records of an individual not subject to agency creation or retention requirements that are created and maintained primarily for the convenience of an agency employee and not distributed to other agency employees for their official use.
- (7) Information stored within a computer for which there is no existing computer software program to extract the information or a printout of the information.
- g. Records management official's duties:
- (1) Army proponent records management duties are specified in paragraph 2–10, DCS, G–1 responsibilities.
- (2) The Director, U.S. Army Records Management and Declassification Agency (USARMDA) has operational responsibility (as determined by the DCS, G–1) for records management and its subprograms as defined in paragraph 8–5. (See AR 25–400–2 for a complete list of duties.)
- (3) MACOM functions pertaining to records management are specified in chapter 2. MACOM records administrators have command-wide responsibilities for ensuring the creation and preservation of official mission records throughout subordinate units and activities. Under ARIMS, the records administrator has the ability to create, modify, and approve office record lists (ORLs) for all subordinate units within the MACOM and can view all of those units' records. Records administrators will—
- (a) Be appointed in writing.
- (b) Provide policy interpretation, procedural guidance, and oversight of mission-unique records management programs.
- (c) Manage, oversee, and direct the records management program and its subprograms.
- (d) Survey and appraise the agency or command records management program at least once every 3 years and prescribe and ensure necessary corrective action is taken.
- (e) Ensure availability of records management training for personnel.
- (f) Oversee, survey, and appraise the methods and operations of records holding areas (RHAs) of the agency or command. Maintain liaison and coordinate records transfer, retirement, and retrieval with Federal Records Centers and local National Archives and Records Administration (NARA) offices.
- (g) Monitor and coordinate records transfer, retirement, and retrieval with central records holding area facilities and the Army Electronic Archives.
- (h) Maintain liaison with and provide advice and assistance to security managers in developing and executing a program to reduce classified records holdings.
- (i) Advise staff and system development personnel on the requirement for integration of records management functions at the concept development stage and coordinate at each milestone. Ensure that records management requirements are documented and included in systems acquisition as appropriate. Keep abreast of and/or implement new IT for access storage, retrieval and disposition of information. Ensure records management factors are considered for the MACOM's C4/IT acquisitions.
- (j) Ensure compliance with the DA Freedom of Information Act Program, the Army Privacy Program, and EO 12958.
- (k) Ensure compliance with and enforcement of DA policies and rules governing management information requirements under the Management Information Control System.
- (l) Maintain liaison with publication, forms, and reports management officials to achieve a minimum production in types and numbers of copies of documents and reports required.
- (m) Provide technical assistance to the VI records managers as required.
- (n) Ensure records management factors are considered for all C4/IT acquisitions.
- (4) MSCs, FOAs, DRUs, separately authorized activities, tenant and satellite organization records managers will—
- (a) Be appointed in writing.
- (b) Approve ORLs for the organization's units.
- (c) Serve as local authority for records management procedures/issues.
- (d) Manage, oversee, and direct the organization's records management program and its subprograms.
- (e) Survey and appraise the organization's records management program at least once every 3 years and prescribe and ensure that necessary corrective action is taken.
- (f) Maintain liaison and coordinate records transfer, retirement, and retrieval with the installation RHA.
- (g) When not served by an installation RHA, index records to be turned in by the organization's offices into the ARIMS Records Input Processing System.
- (h) Ensure records are properly arranged and packed prior to movement from the organization to a records center. Maintain liaison and coordinate records transfer, retirement, and retrieval with the National Records Center facilities and local NARA offices.

- (i) Ensure availability of training for records management personnel.
- (j) Maintain liaison with and provide advice and assistance to security managers in developing and executing a program to reduce classified records holdings to the absolute minimum required.
- (k) Provide technical assistance to VI records managers.
- (5) IMA will provide program coordination to the regional records managers, as required.
- (6) Regional-level records managers will—
  - (a) Provide functional management and oversight of the records management program and its subprograms for the installations in their respective regions in accordance with AR 25–400–2, AR 25–55, AR 340–21, DA Pam 25–51, AR 380–5, AR 25–50, AR 310–4, AR 335–15, AR 310–25, AR 310–50, and DA Pam 25–50.
  - (b) Regional mail managers will execute the official mail cost control program in their respective regions per AR 25–51.
- (7) Installation-level records managers serve on the installation staff and have installation-wide responsibilities. They will—
  - (a) Be appointed in writing.
  - (b) Approve ORLs for subunits.
  - (c) Serve as local authority for records management procedures/issues.
  - (d) Manage, oversee, and direct the installation records management program and its subprograms.
  - (e) Survey and appraise the installation's records management program at least once every 3 years and prescribe and ensure that necessary corrective action is taken.
  - (f) Manage and provide staff direction for the operation of the RHA. Ensure records are properly arranged and packed prior to movement from the records holding area to a records center. Maintain liaison and coordinate records transfer, retirement, and retrieval with the Federal Records Centers and local NARA offices. Index records turned in by installation offices and tenant offices into the ARIMS Records Input Processing System.
  - (g) Ensure that records management factors are considered for all installation level IT/C4I acquisitions.
  - (h) Ensure availability of training for records management personnel.
  - (i) Maintain liaison with and provide advice and assistance to security managers in developing and executing a program to reduce classified records holdings to the absolute minimum required.
  - (j) Provide technical assistance to VI records managers, as required. Installation mail managers will execute the official mail cost-control program throughout the installation per AR 25–51.
- (8) Records coordinators will be designated at subelements as necessary for program execution. Coordinators will perform records management duties as assigned:
  - (a) Develop ORL for their unit.
  - (b) Coordinate transfer of T (long-term/permanent) records to the installation or central RHA.
  - (c) Serve as the subject matter expert for the unit's records.
  - (d) Resolve indexing problems with the contractor.
  - (e) Perform other records management duties as assigned.
- (9) An action officer is any individual who creates official records on behalf of the Army. The action officer (at all levels of command) has the capability to search the Army's office record instructions to help determine if a document is an official record, create a draft ORL to be maintained for each office symbol within a unit or organization, submit records to a designated records holding facility, and search for and request records in ARIMS. The action officer can also view all records submitted to ARIMS internal to the unit. In addition, the action officer identifies records as K (short-term) or T and, for e-records, registers in ARIMS, and submits records via the e-mail capture and store feature of ARIMS.

### **8–3. Life-cycle management of records**

- a. Maintaining Army information that meets the definition of a record is the responsibility of all military, civilian, and contractor personnel, commanders, and leaders (See AR 25–400–2, chap 6, on how to maintain official records). Create only the minimum records essential and adequate to support, sustain, and document the following:
  - (1) Military operations in time of peace, war, and operations other than war (for example, contingency operations and humanitarian, peacekeeping, and nation building missions).
  - (2) The conduct of all other activities of the Army's official business.
- b. Protect the rights and interests of the Army, its uniformed members and their dependents, civilian employees, and affiliated personnel.
- c. Control the quantity and quality of records produced by the Army.
- d. Establish and maintain control of the creation of data elements to be placed in records so the information contributes to the effective and economical operations of the Army and prevent the creation of unnecessary records.
- e. Simplify the activities, systems, and processes of record creation and of record maintenance and use.
- f. Direct continuing attention to the life-cycle management of information from initial creation to final disposition.

- g. Establish and maintain such other systems or techniques as the Archivist of the United States, in consultation with the Archivist of the Army, finds necessary.
- h. Employ modern technologies and cost effective provide alternatives for storage, retrieval, and use of records.
- i. Ensure records are preserved in a manner and on media that meet all legal and archival requirements.
- j. Incorporate standards and technical specifications in all information systems' functional requirements to ensure the life-cycle management of record information.
- k. Ensure the periodic evaluation of the records management activities relating to the adequacy of documentation, maintenance and use, and records disposition, at all levels, through the information resources management review process.

#### **8-4. Tenets**

In executing the mission, objectives, and subprograms, Army activities will conform to the following program tenets:

- a. Simplify recordkeeping methods.
- b. Minimize the burden on commanders, soldiers, and civilian and contractor personnel.
- c. Establish proactive control over operational records.
- d. Centralize record collection when deployed in theater.
- e. Digitize once with multiple access.
- f. Ensure appropriate command emphasis.
- g. Incorporate records management requirements into training.

#### **8-5. Major subprograms**

a. *Army recordkeeping systems management.* The objectives of Army recordkeeping systems management are to cost-effectively organize Army records stored on any medium so needed records can be found rapidly; to ensure that records are complete, accurate, authentic, reliable, and trustworthy; to facilitate the selection and retention of records of enduring value; and to accomplish the prompt disposition of noncurrent records in accordance with NARA-approved disposition schedules. (See AR 25-400-2.)

(1) *ARIMS.* The ARIMS provides policy and procedures for the systematic identification, maintenance, retirement, and destruction of Army record information. It provides for the establishment and operation of central and overseas command records holding areas, and furnishes the legal authority for destruction of nonpermanent Army records by organizational elements. ARIMS replaces the Modern Army Records Keeping System (MARKS).

(2) *Electronic recordkeeping systems.* Electronic recordkeeping systems collect, organize, and categorize records to facilitate their preservation, retrieval, use, and disposition. These systems may include audio, e-mail, office automation software applications, databases, and visual and image information systems utilizing IT.

(3) *Manual recordkeeping systems.* Life-cycle management of information contained in manual information systems includes paper, image, audio, photo, and visual information.

b. *Official mail and distribution management.*

(1) Official mail and distribution management provides rapid handling and accurate delivery of official mail throughout the Army at minimum cost. To do this and to increase efficiency, processing steps are kept to a necessary minimum; sound principles of workflow are applied; modern equipment, supplies, and devices are used; and operations are kept as simple as possible. This subprogram includes responsibility for ZIP+4 addressing and office symbols. (See AR 25-51.)

(2) Office symbols are used to identify originators of correspondence and electronically transmitted messages and to denote the proper placement of Army organizations in the Army structure for historical and records purposes. They are also used as part of the address when forwarding correspondence and mail to, from, or within HQDA. Office symbols will be as short as possible. Office symbols should be added or deleted when new organizational elements are created, existing organizational elements are terminated, or organizational elements are divided or merged. The first two letters of an office symbol indicate the organization's primary command. "SA" is reserved for OSA or an OSA activity; "DA" for other HQDA staff elements. Office symbols of HQDA FOAs, staff support agencies, and DRUs will begin with two letters representing the parent staff agency.

(3) The basic office symbol for MACOMs will be constructed using the HQDA construction method and assigned by the U.S. Army Records Management and Declassification Agency. (See <https://www.arims.army.mil> for procedures.) The AASA (for the Secretariat and ARSTAF) and MACOMs will submit their requests for deletions, additions, and corrections to the U.S. Army Records Management and Declassification Agency, ATTN: AHRC-PDD-RP, 7701 Telegraph Rd, Rm 102, Alexandria, VA 22315-3860. Other units and activities will submit to their next-higher headquarters.

(4) Requests for exceptions to the HQDA construction standards as outlined in the USARMDA Web site <https://www.arims.army.mil> will be submitted through the organization's chain of command to USARMDA for approval.

c. *Correspondence management.* The correspondence management program provides for the preparation and management of correspondence in a standardized, economical, and efficient manner. (See AR 25-50.)

*d. Rulemaking.* The rulemaking program satisfies the legal requirement for the Army to publish, in the Federal Register, Army regulations or other issuances and notices that have a substantial and continuing impact on the public. (See AR 310-4.)

*e. FOIA program management.* The FOIA program implements the DOD policy that requires its activities to conduct business in an open manner and to provide the public a maximum amount of accurate and timely information concerning its activities, consistent with legitimate public and private interests of the American people. (See AR 25-55.)

*f. Privacy Act program management.* The Privacy Act program provides a comprehensive framework regulating how DA collects, maintains, uses, or disseminates personal information on individuals. The program provides balance between information requirements of the Department and privacy interests and concerns of the individual. (See AR 340-21 and DA Pam 25-51.)

*g. Management Information Control Office (MICO).* The HQDA MICO objectives are to establish policy, procedures and standards for IM control and prescribe responsibilities for the management and control of external and internal Army information requirements. These objectives include interpreting and implementing existing Army reports control policy, statutes and external guidance (OMB, GSA, and DOD); implementing Army information control policy goals and objectives; and assigning requirement control symbols (RCSs). The MICO will evaluate proposed, new, or revised public information requirements; prepare the Annual Information Collection Budget; and plan and coordinate periodic reviews of Army IM requirements, IT products, and public information requirements. (See AR 335-15.)

*h. Vital records.* This program provides for the selection and protection of records required for the Army to conduct its business under other than normal operating conditions, to resume normal business afterward, and to identify and protect important records dealing with the legal and financial rights of the Army and persons directly affected by actions of the Army. It also provides policies and guidance for emergency preparedness, contingency planning, assessing damage, and implementing disaster recovery procedures.

(1) *Emergency operating records.* These are records essential to the continued functioning and reconstitution of an organization before, during, and after a national security emergency or under emergency or disaster conditions. These records include such groups as emergency plans and mobilization plans and programs. Per AR 500-3, HQDA, MACOMs, and certain activities maintain copies of emergency operating records at predesignated relocation and alternate sites. (See also para 6-1b.)

(2) *Rights and interests records.* These are records essential to the preservation of the legal and financial rights and interests of individual citizens and the Army (including its Service members). These records include retirement records; finance and accounting records; medical records; payroll records; personnel action records; certain records from operational deployments; records related to contracts, entitlements, and/or leases; and other valuable research records.

*i. Terminology, abbreviations, and brevity code management.* The Terminology Standardization Management Program contains two interrelated areas:

(1) *Dictionary of Army Terms.* This program is designed to assist in reaching a more-common understanding of the meaning of terminology used extensively by the U.S. Army and with the DOD and International Standardization usage. (See also AR 310-25.)

(2) *Authorized abbreviation and brevity codes.* This program prescribes authorized abbreviations and brevity codes and procedures for their use within the Army. Program objectives are to standardize abbreviations and brevity codes used within DOD and between DOD elements and NATO countries and assist in reaching a mutual or common definition and meaning of terminology between DOD elements, and between DOD elements and NATO member countries.

*j. Management of records of defunct Army commands and organizations.* This subprogram manages records from Army organizations that no longer exist. Such records are in the physical custody of a Federal Records Repository but are still under Army control awaiting transfer of legal authority over the records to the National Archives.

*k. Oversight records administration of Joint/multi-Service/DOD.* These are records that have been transferred into a Federal Records Repository and for which DOD has designated the Army as executive agency for record administration until legal authority is transferred to the National Archives.

*l. Archivist of the Army.* The DCS, G-1 is the Archivist of the Army and is responsible for the senior coordination and interface with the Archivist of the United States. The Army Archivist may delegate specific responsibilities for achieving the records management mission. The recipients of such delegation are effectively assistant archivists of the Army. The Archivist of the Army promotes cooperation with the Archivist of the United States in applying standards, procedures, techniques, and schedules designed to improve management of records, safeguard the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and disposal of records of temporary value. The Archivist of the Army takes final action to offer records to NARA. Standard Form (SF) 258 (Agreement to Transfer Records to the National Archives of the United States) is used to offer Army records formally to the Archivist of the United States and to accession records into the National Archives. Use of SF 258 is limited to DCS, G-1 (DAPE-ZXI-RM) or as designated by the DCS, G-1.

*m. Defense Visual Information Center (DVIC).* The DVIC is the only authorized VI record center for OSD and the

military components. Official record material is submitted to the DVIC through the JVISDA or through the CAP. (See also para 7–10.)

*n. Armed Services Center for Unit Records Research Program.* The program meets current and future Army requirements by locating, analyzing, and extracting pertinent data from unit records created during U.S. military operations past and present. The program provides expertise in the identification and interpretation of pertinent U.S. Army combat unit records for the purpose of verifying the claims of veterans, supporting scientific and epidemiological studies, and creating and maintaining databases associated with the total military combat experience.

## **8–6. General policies**

*a.* Personal papers pertain solely to an individual's private affairs. Official records are made or received in compliance with Federal law in the transaction of public business. Correspondence designated personal, private, eyes only, and so on, but relevant to the conduct of public business, are official records. Back-channel messages are official records that are processed under stricter handling and transmission techniques than normal message traffic. All official records are subject to life-cycle management procedures and are the property of the Federal Government, not the military member or employee making or receiving them.

*b.* For convenience of reference, a Government official may accumulate extra copies of records that they have drafted, reviewed, or otherwise acted upon while in office. When deposited in a recognized research institution, these reference files or by-name collections often serve the broader interests of historiography. These reference files commonly are invaluable to later generations of staff planners and historians in discovering the rationales of the decision process. Government officials may accumulate these extra copies, if this action does not—

- (1) Diminish the official records of the agency.
- (2) Violate national security or confidentiality required by privacy or other interests protected by law.
- (3) Exceed normal administrative costs.

*c.* Army general officers and senior civilian executives (normally limited to SES grades) may place reference files that they create during their tenure of office with the Military History Institute without violating the prohibitions discussed above. Moreover, such donations create a single source of information on actions accomplished by high-level officials. The Director of the Military History Institute will preserve the integrity of these collections with the identification of the donor, such as the "Abrams Papers," or the "Bradley Papers." During the donors' lifetimes, their own collections will be open to them for research, reference, or historical inquiry. The Director of the Military History Institute will provide archival and librarian assistance to the donor. The donor must meet the security clearance requirements of AR 380–5.

*d.* Records identified below may not be removed from the control of the Federal Government for personal retention or donation to any institution unless approval is obtained from the Archivist of the United States:

- (1) The official record copy of any document.
- (2) Security classified documents.
- (3) Restricted data or formerly restricted data documents (AR 380–5).
- (4) Diaries that contain official schedules of meetings, appointments, field trips, or other official activities. These are official records and will be so maintained.
- (5) Copies of records containing information exempted from public release under the nine exemptions of the Freedom of Information Act or the Privacy Act.
- (6) Any record, including any normally nonrecord copy, whose absence creates a gap in the files or impairs the logical sequence of essential documentation.
- (7) Records required to transact the official business of the Army and any document that assists in the decision-making process.
- (8) Records identified below may be removed when the individual creating them retires, resigns, or otherwise terminates his or her tenure of office.

*(a)* All personal and private papers that do not contain references to official business.

*(b)* Personal diaries, logs, notes, memoranda, tapes, disks, and summaries of telephone conversations, if all official information has been duplicated in official memoranda for record for retention in the official files.

*(c)* Reference books and other personal items brought from private life.

*e.* Separation and control of personal papers at the time of creation is the best way to avoid mixing personal papers with official records.

*f.* Commanders and agency heads will safeguard official records and properly dispose of them, per policy guidance in this regulation and in AR 25–400–2. Safeguarding against the removal or loss of Federal records includes an annual, locally developed, mandatory briefing of all military, civilian, and contractor personnel to ensure that all DA personnel are aware that—

- (1) Transfer of title and destruction of records in the custody of the Army are governed by specific provisions of 44 USC, Chapter 33.



(2) There are criminal penalties for the unlawful removal or destruction of Federal records and for the unlawful disclosure of information pertaining to national security and personal privacy (AR 25-400-2, AR 340-21, AR 380-5).

(3) Under the Federal Records Act of 1950, records in the custody of the Army OCONUS may be destroyed at any time during the existence of a state of war between the United States and any other power; or when hostile action by a foreign power appears imminent, if their potential capture by the enemy is prejudicial to the interests of the United States. If emergency destruction is done, a list of records destroyed, their inclusive dates, and the date destroyed will be compiled as much as possible. This information will be forwarded through channels to the U.S. Army Records Management and Declassification Agency, ATTN: AHRC-PDD-R, Stop 5603, 6000 6th Street, Fort Belvoir, VA 22060-5603, as expeditiously as theater or operational conditions permit.

g. All Army users are reminded that one AKM goal is to actively seek ways to identify, catalog, file, search, and retrieve data (that is, records). Commanders must discourage hoarding of information by subordinates and instead encourage creation of internal business processes, Web sites, relational databases, repositories, or libraries of related information for all command users and eventually all qualified Army users with a need to know to access.

## **8-7. Record media**

a. Information created within the Army may be recorded on various display media such as paper, microform, machine-readable format, or presentation media (audio and visual). Approved Army disposition schedules (see AR 25-400-2) apply to all Army recorded information regardless of the media upon which recorded. In order to protect the rights and interests of the Army and its members, keep costs to a minimum, and serve the study of history, display or presentation media for long-term records that best serve the operational needs of the Army and meet statutory scheduling requirements must be selected. These decisions are vital considerations in the design stage of information life-cycle management.

b. When other than paper is the record copy—

(1) The medium selected must have the durability to meet the test of time established by the ARIMS records retention schedule—Army, such as retention period for the information contained in the system, individual microform or database. AR 25-400-2 provides policy for the systematic identification, maintenance, retirement, and destruction of Army record information. Where more than one ARIMS file series is contained in the record, systems of records, or database, the longest included retention schedule will apply. Electronic records management automated information systems will comply with DOD 5015.2-STD.

(2) The ability to retrieve record information economically and efficiently must be maintained for the length of time that the information remains in the Army's legal custody. Army records retired to Federal Records Centers remain in Army legal custody even though they are in the physical custody of NARA. Formal accessioning into the National Archives of the United States, however, transfers legal custody from the Army to the Archivist of the United States.

(3) Federal Records Centers have storage facilities for records stored in machine-readable and microform media; however, they do not possess servicing capability. The retiring activity for servicing, testing, manipulation, or data processing must retrieve records in these media.

(4) Information retained as the record copy on other than paper must meet all legal requirements imposed on the records of the Federal Government and must adequately protect the rights and interests of both the Army and any individual members, dependents, employees, or citizens that it affects.

(5) VI original materials are retained in their original format.

(6) When microforms are the recording media for permanent records, silver halide film must be employed. For records that do not have a permanent retention requirement, the original microform can be either dry silver or silver halide, and the choice is dependent upon which provides the most efficient and economical filming process. The original microform copy normally will be used only to make either diazo or vesicular duplicates. Duplicate microforms will be used for current day-to-day reference or operations, as they are more economical and scratch resistant than the original microform.

(7) When the record copy from an information system is converted to a microform document, the longest retention of any ARIMS record series contained in the microform will determine the technical specifications of the film to be used. It is the responsibility of the appropriate information manager to ensure that the type of film used meets established retention requirements. If the document being converted to microform contains a permanent ARIMS record series as determined by the Archivist of the United States, special conditions noted in *c*, below, apply.

(8) When the permanent record copy is on microform, an archival film test (sometimes called the methylene blue technique) is required to ensure damaging chemicals that will deteriorate the recorded information are not retained on the film. In addition to the film test, all microforms produced will conform to quality standards and formats.

c. The Archivist of the United States has proprietary interest in the permanent records of DA (and all other Federal agencies). This covers the entire life cycle from creation until eventual deposit in the National Archives. This proprietary interest includes both the informational contents of the records and the recording and storage media.

(1) Prior to converting a permanent series of records to microform, a specific determination must be solicited from the Archivist of the United States. In some instances, the filmed documents are not acceptable for deposit in the National Archives, and the original media must be provided.

(2) Agencies may use optical media for storage and retrieval of permanent records while the records remain in an agency's legal custody. However, permanent records may not be destroyed after copying onto optical media without NARA's approval. Requests should be sent to the U.S. Army Records Management and Declassification Agency, address at paragraph 8-6f.

*d.* Due to personal health risks, agencies will not destroy optical media (CDs, DVDs) by burning, pulverizing, or shredding. Optical media will be stored pending development of final disposition instructions. If the volume of stored optical media becomes a storage or security concern, the manufacturer should be contacted to seek assurance that the product does not contain toxic substances. With manufacturer assurance relating to specific disk products, excess optical media may be smelted.

#### **8-8. Electronic records management**

*a.* Army records, regardless of media or format, must follow the disposition instructions identified in AR 25-400-2 and comply with the security requirements of AR 25-2. All electronic information generated by or contained in an information system or any office IT source, or created during the conduct of electronic business/electronic commerce, must be considered. This requirement applies to information contained in any enterprise information system, e-mail, command unique systems, and systems maintained in the office environment. The disposition of electronic records must be determined as early as possible in the life cycle of the information system.

*b.* VI digital still and motion images are excluded from this paragraph. VI products are managed under the provisions of DODI 5040.6, chapter 7 of this regulation, and DA Pam 25-91.

## **Appendix A References**

### **Section I Required Publications**

#### **AR 5–20**

Commercial Activities Program. (Cited in paras 6–2*c*(1) and 7–3*c*(6).)

#### **AR 25–2**

Information Assurance. (Cited in paras 1–7, 1–8, 2–16*g*, 2–27*a*(6), 4–7*h*, 5–1*a*, 5–3*c*, 5–4, 5–5*b*, 5–5*c*, 5–7*c*, 5–8*c*, 6–1*g*, 6–1*i*, 6–4*q*, 6–4*r*, 6–4*cc*, 7–8*a*(6)(*b*)16, and 8–8*a*.)

#### **AR 25–30**

The Army Publishing Program. (Cited in paras 7–7*a*, 9–1, and 9–4.)

#### **AR 25–55**

The Department of the Army Freedom of Information Act Program. (Cited in paras 1–7, 7–12*i*, 7–12*l*, 8–2*f*, 8–2*g*(6), and 8–5*e*.)

#### **AR 25–400–2**

The Army Records Information Management System (ARIMS). (Cited in paras 1–5, 2–12*i*, 2–24, 6–1*c*, 6–4*m*(10), 7–10*a*, 7–12*l*, 8–2*d*(4), 8–2*g*(2), 8–2*g*(6), 8–3*a*, 8–5*a*, 8–6*f*, 8–7*a*, 8–7*b*, and 8–8*a*.)

#### **AR 70–1**

Army Acquisition Policy. (Cited in paras 2–5, 2–16*c*, 3–2*b*(4), 3–7, 6–1*n*(2), 6–2*g*(8), 6–5*i*, and 7–2*h*.)

#### **AR 71–9**

Materiel Requirements. (Cited in paras 2–16*c*, 3–4*f*, 3–5*a*(1), 3–6*d*, 3–7, 6–5*i*, 7–2*h*, and B–4*b*(17).)

#### **AR 215–1**

Morale, Welfare, and Recreation Activities and Nonappropriated Fund Instrumentalities. (Cited in paras 6–1*n*, 6–4*o*, and 6–4*s*.)

#### **AR 215–4**

Nonappropriated Fund Contracting. (Cited in paras 6–1*n*(2) and 6–4*o*.)

#### **AR 340–21**

The Army Privacy Program. (Cited in paras 1–7, 7–12*i*, 7–12*l*, 8–2*g*(6), 8–5*f*, and 8–6*f*.)

#### **AR 360–1**

The Army Public Affairs Program. (Cited in paras 6–4*n*(4) and 6–4*s*(6)(*f*).)

#### **AR 380–5**

Department of the Army Information Security Program. (Cited in paras 4–7*h*, 7–8*a*(6)(*b*)16, 7–12*i*, 8–2*g*(6), 8–6*c*, 8–6*d*(3), and 8–6*f*.)

#### **AR 380–53**

Information Systems Security Monitoring. (Cited in paras 6–4*q* and 6–4*r*.)

#### **DA Pam 25–1–1**

Installation Information Services. (Cited in paras 6–2*k*(3) and 8–5.)

#### **DA Pam 25–91**

Visual Information Procedures. (Cited in paras 7–4*e*, 7–5*e*, 7–7*c*(1), 7–7*e*, 7–8*a*(6), 7–8*b*(1), 7–10*a*, 7–10*b*, 7–11*a*, 7–11*b*, 7–12*i*, and 8–8*b*.)

#### **DOD 5500.7–R**

Joint Ethics Regulation (JER). (Cited in paras 1–8 and 6–1*d*(1).) (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 1015.14**

Establishment, Management, and Control of Nonappropriated Fund Instrumentalities. (Cited in para 6–1*n*.) (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 5040.2**

Visual Information (VI). (Cited in paras 2–1*o*, 7–7*c*(2)(*a*), and 7–12*b*.) (Available at <http://www.dtic.mil/whs/directives>.)

**DODI 4640.14**

Base and Long-Haul Telecommunications Equipment and Services. (Cited in para 6–5*a*(1).) (Available at <http://www.dtic.mil/whs/directives>.)

**DODI 5000.2**

Operation of the Defense Acquisition System. (Cited in paras 2–5*g* and 3–7*b*(2).) (Available at <http://www.dtic.mil/whs/directives>.)

**DODI 5200.40**

DOD Information Technology Security Certification and Accreditation Process (DITSCAP). (Cited in paras 5–3*b*, 5–3*c*, and 5–5*c*.) (Available at <http://www.dtic.mil/whs/directives>.)

**29 U.S.C. 794d**

Section 508 of the Rehabilitation Act Amendments of 1998, as amended by Section 2405 of the FY 2001 Military Appropriations Act (P.L. 105–220). (Cited in para 6–4*n*(13).) (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**P.L. 107–347**

E–Government Act of 2002 (Cited in paras 2–1*e*(8) and 3–9*c*.) (Available at <http://www.gpoaccess.gov/plaws/index.html>.)

**Section II****Related Publications**

A related publication is a source of additional information. The user does not have to read the publication to understand this regulation.

**ACP 123(A)**

Common Messaging Strategy and Procedures. (Available at <http://www.dtic.mil/jcs/j6/cceb/acps/>.)

**AR 5–11**

Management of Army Models and Simulations

**AR 5–12**

Army Management of the Electromagnetic Spectrum

**AR 5–22**

The Army Proponent System

**AR 10–5**

Headquarters, Department of the Army

**AR 12–8**

Operations and Procedures

**AR 25–6**

Military Affiliate Radio System (MARS)

**AR 25–50**

Preparing and Managing Correspondence

**AR 25–51**

Official Mail and Distribution Management

**AR 27–26**

Rules Of Professional Conduct For Lawyers

**AR 27–60**

Intellectual Property

**AR 71–32**

Force Development and Documentation—Consolidated Policies

**AR 105–70**

Amateur Radio Operations

**AR 115–11**

Geospatial Information and Services

**AR 190–53**

Interception of Wire and Oral Communications for Law Enforcement Purposes

**AR 310–4**

Publication in the Federal Register of Rules Affecting the Public

**AR 310–25**

Dictionary of United States Army Terms

**AR 310–50**

Authorized Abbreviations, Brevity Codes, and Acronyms

**AR 335–15**

Management Information Control System

**AR 340–26**

Duplicate Emergency Files Program

**AR 380–10**

Foreign Disclosure and Contacts with Foreign Representatives

**AR 380–40 (O)**

Policy for Safeguarding and Controlling Communications Security (COMSEC) Material (U)

**AR 380–381**

Special Access Programs (SAPs)

**AR 381–14 (C)**

Technical Counterintelligence (TCI) (U)

**AR 415–15**

Army Military Construction Program Development and Execution

**AR 500–3**

Army Continuity of Operations (COOP) Program

**AR 600–7**

Nondiscrimination on the Basis of Handicap in Programs and Activities Assisted or Conducted by the Department of the Army

**AR 640–30**

Photographs for Military Personnel Files

**AR 700–127**

Integrated Logistics Support

**AR 700-131**

Loan and Lease of Army Material

**AR 700-142**

Materiel Release, Fielding, and Transfer

**AR 710-2**

Supply Policy Below the National Level

**AR 735-5**

Policies and Procedures for Property Accountability

**AR 750-1**

Army Materiel Maintenance Policy

**CJCSI 3170.01D**

Joint Capabilities Integration and Development System. (Available at [http://www.dtic.mil/cjcs\\_directives](http://www.dtic.mil/cjcs_directives).)

**CJCSI 6110.01A**

CJCS-Controlled Tactical Communications Assets. (Available at [http://www.dtic.mil/cjcs\\_directives](http://www.dtic.mil/cjcs_directives).)

**CJCSI 6212.01C**

Interoperability and Supportability of Information Technology and National Security Systems. (Available at [http://www.dtic.mil/cjcs\\_directives](http://www.dtic.mil/cjcs_directives).)

**CJCSI 6215.01B**

Policy for Department of Defense Voice Networks. (Available at [http://www.dtic.mil/cjcs\\_directives](http://www.dtic.mil/cjcs_directives).)

**CJCSI 6250.01A**

Satellite Communications. (Available at [http://www.dtic.mil/cjcs\\_directives](http://www.dtic.mil/cjcs_directives).)

**CTA 50-909**

Field and Garrison Furnishings and Equipment

**DA Pam 25-30**

Consolidated Index of Army Publications and Blank Forms

**DA Pam 25-40**

Army Publishing: Action Officers Guide

**DA Pam 25-50**

Compilation of Army Addresses

**DA Pam 25-51**

The Army Privacy Program-System of Records Notices and Exemption Rules

**DA Pam 70-3**

Army Acquisition Procedures

**DA Pam 700-142**

Instructions for Materiel Release, Fielding, and Transfer

**DCID 6/3**

Protecting Sensitive Compartmented Information Within Information Systems. (Available at [http://www.us.army.mil/portal/portal\\_home.jhtml](http://www.us.army.mil/portal/portal_home.jhtml).)

**DFARS Subpart 208.74**

Enterprise Software Agreements. (Available at <http://www.acq.osd.mil/dpap/dfars/index.htm>.)

**DFAS-IN Regulation 37-1**

Finance and Accounting Policy Implementation. (Available at <http://www.asafm.army.mil/budget/di/di.asp>.)

**DISA Circular 310-130-1**

Submission of Telecommunications Service Requests. (Available at Web site <https://disa-ca.dtic.mil/pubs>.)

**DISA Circular 310-130-4**

Defense User's Guide to the Telecommunications Service Priority (TSP) System. (Available at Web site <https://disa-ca.dtic.mil/pubs>.)

**DOD 4160.21-M**

Defense Materiel Disposition Manual. (Available at <http://www.dtic.mil/whs/directives>.)

**DOD 4525.8-M**

DOD Official Mail Manual. (Available at <http://www.dtic.mil/whs/directives>.)

**DOD 5015.2-STD**

Design Criteria Standard for Electronic Records Management Software Applications. (Available at <http://www.dtic.mil/whs/directives>.)

**DOD 5200.2-R**

Personnel Security Program. (Available at <http://www.dtic.mil/whs/directives>.)

**DOD 5400.7-R**

DOD Freedom of Information Act Program. (Available at <http://www.dtic.mil/whs/directives>.)

**DOD 7000.14-R (vol. 2B, chap. 18)**

Department of Defense Financial Management Regulations (FMRs) (Information Technology/National Security Systems). (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 1015.2**

Military Morale, Welfare, and Recreation (MWR). (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 1035.1**

Telework Policy for Department of Defense. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 3020.26**

Continuity of Operations (COOP) Policy and Planning. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 4630.5**

Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS). (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 4640.1**

Telephone Monitoring and Recording. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 4640.7**

DOD Telecommunications System (DTS) in the National Capital Region (NCR). (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 4640.13**

Management of Base and Long-Haul Telecommunications Equipment and Services. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 5015.2**

DOD Records Management Program. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 5025.1**

DOD Directives System. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 5025.12**

Standardization of Military and Associated Terminology. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 5040.3**

DOD Joint Visual Information Services. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 5040.4**

Joint Combat Camera (COMCAM) Program. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 5040.5**

Alteration of Official DOD Imagery. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 5230.9**

Clearance of DOD Information for Public Release. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 5400.11**

DOD Privacy Program. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 5530.3**

International Agreements. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 7950.1**

Automated Data Processing Resources Management. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 8000.1**

Management of DOD Information Resources and Information Technology. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 8100.1**

Global Information Grid (GIG) Overarching Policy. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 8190.2**

The Department of Defense (DOD) Electronic Business/Electronic Commerce (EB/EC) Program. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 8190.3**

Smart Card Technology. (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 8500.1**

Information Assurance (IA). (Available at <http://www.dtic.mil/whs/directives>.)

**DODD 8910.1**

Management and Control of Information Requirements. (Available at <http://www.dtic.mil/whs/directives>.)

**DODI 1000.15**

Private Organizations on DOD Installations. (Available at <http://www.dtic.mil/whs/directives>.)

**DODI 1015.12**

Lodging Program Resource Management. (Available at <http://www.dtic.mil/whs/directives>.)

**DODI 4000.19**

Interservice and Intragovernmental Support. (Available at <http://www.dtic.mil/whs/directives>.)

**DODI 5040.6**

Life-Cycle Management of DOD Visual Information (VI). (Available at <http://www.dtic.mil/whs/directives>.)

**DODI 5040.7**

Visual Information (VI) Production Procedures. (Available at <http://www.dtic.mil/whs/directives>.)



**DODI 5330.2**

Specifications for DOD Letterheads. (Available at <http://www.dtic.mil/whs/directives/>.)

**DODI 5335.1**

Telecommunications Services in the National Capital Region (NCR). (Available at <http://www.dtic.mil/whs/directives/>.)

**DRMS Instruction 4160.14, Volume IV**

Policy and Procedures In Disposal Operations for Property Accounting. (Available at <http://www.drms.dla.mil/publications/index.html>.)

**Executive Order 12600**

Predisclosure Notification Procedures for Confidential Commercial Information. (Available at [http://www.archives.gov/federal\\_register/executive\\_orders/disposition\\_tables.html](http://www.archives.gov/federal_register/executive_orders/disposition_tables.html).)

**Executive Order 12845**

Requiring Agencies to Purchase Energy Efficient Computer Equipment. (Available at [http://www.archives.gov/federal\\_register/executive\\_orders/disposition\\_tables.html](http://www.archives.gov/federal_register/executive_orders/disposition_tables.html).)

**Executive Order 12958**

Classified National Security Information. (Available at [http://www.archives.gov/federal\\_register/executive\\_orders/disposition\\_tables.html](http://www.archives.gov/federal_register/executive_orders/disposition_tables.html).)

**Executive Order 12999**

Educational Technology: Ensuring Opportunity for all Children in the Next Century. (Available at [http://www.archives.gov/federal\\_register/executive\\_orders/disposition\\_tables.html](http://www.archives.gov/federal_register/executive_orders/disposition_tables.html).)

**Executive Order 13011**

Federal Information Technology. (Available at [http://www.archives.gov/federal\\_register/executive\\_orders/disposition\\_tables.html](http://www.archives.gov/federal_register/executive_orders/disposition_tables.html).)

**Executive Order 13103**

Computer Software Piracy. (Available at [http://www.archives.gov/federal\\_register/executive\\_orders/disposition\\_tables.html](http://www.archives.gov/federal_register/executive_orders/disposition_tables.html).)

**Federal Acquisition Regulation**

Government Printing and Binding Regulations. (Available at <http://www.arnet.gov/far/>.)

**FM 6-02.40**

Visual Information Operations

**General Order 1997-23**

Transfer of Publications and Printing

**General Order 1997-24**

Transfer of Records Management

**General Records Schedule 21**

Audiovisual Records, Transmittal No. 8, December 1998. (Available at [http://www.archives.gov/records\\_management/ardot/](http://www.archives.gov/records_management/ardot/).)

**JCS 1-02**

Department of Defense Dictionary of Military and Associated Terms. (Available at [http://www.dtic.mil/doctrine/jel/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf).)

**Joint Travel Regulations**

(Available at <http://www.dtic.mil/perdiem/trvlregs.html>.)

**National Security Decision Directive 145**

National Policy on Telecommunications and Automated Information Systems Security. (Available at <http://www.fas.org/irp/offdocs/direct.htm>.)

**National Security Directive 42**

National Policy for the Security of National Security Telecommunications and Information Systems. (Available at <http://www.fas.org/irp/offdocs/direct.htm>.)

**NSTISSD No. 900, Section IV (Responsibilities)**

Governing Procedures of the National Telecommunications and Information Systems Security Committee (NSTISSC). (Available at <http://www.nstissc.gov/>.)

**NSTISSP No. 11**

National Information Assurance Acquisition Policy. (Available at <http://www.nstissc.gov/>.)

**OMB Cir A-11**

Preparation, Submission, and Execution of the Budget. (Available at <http://www.whitehouse.gov/omb/circulars/index.html>.)

**OMB Cir A-76**

Performance of Commercial Activities. (Available at <http://www.whitehouse.gov/omb/circulars/index.html>.)

**OMB Cir A-109**

Major Systems Acquisitions. (Obtain hard copy (only) from the Office of Management and Budget, telephone (202) 395-3080.)

**OMB Cir A-130**

Management of Federal Information Resources. (Available at <http://www.whitehouse.gov/omb/circulars/index.html>.)

**P.L. 92-463**

Federal Advisory Committee Act. (Available at [http://www.epic.org/open\\_gov/faca.html](http://www.epic.org/open_gov/faca.html).)

**P.L. 97-375**

Congressional Reports Elimination Act of 1982. (Available at <http://thomas.loc.gov/bss>.)

**P.L. 104-106 (40 USC 1401 et seq.)**

The Clinger-Cohen Act of 1996 (formerly Div E, Information Technology Management Reform Act, Defense Authorization Act of 1996). (Available at <http://www.gpoaccess.gov/plaws/index.html>.)

**P.L. 104-191**

Health Insurance Portability and Accountability Act of 1996 (HIPAA). (Available at <http://www.gpoaccess.gov/plaws/index.html>.)

**P.L. 105-220**

Rehabilitation Act Amendments of 1998. (Available at <http://www.gpoaccess.gov/plaws/index.html>.)

**P.L. 105-277**

The Government Paperwork Elimination Act (Div. C, Title XVII 112 STAT, 2681-751, Oct 21, 1998). (Available at <http://www.gpoaccess.gov/plaws/index.html>.)

**P.L. 106-398**

Government Information Security Reform Act (Title X, Subtitle G of the 2001 Defense Authorization Act (Sections 1061-1065)). (Available at <http://www.gpoaccess.gov/plaws/index.html>.)

**P.L. 106-554**

Federal Information Quality Act (Section 515, FY 2001 Treasury and General Government Appropriations Act). (Available at <http://www.gpoaccess.gov/plaws/index.html>.)

**SB 700-20 (EM 0007 FEDLOG)**

Army Adopted/Other Items Selected for Authorizations/List of Reportable Items. (Available at <http://weblob.logsa.army.mil/index.shtml>.)

**36 CFR Chapter 7**

Chapter 7, Library of Congress. (Available at <http://www.gpoaccess.gov/cfr/index.html>.)

**5 USC 552**

Freedom of Information Act. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**5 USC 552a**

The Privacy Act. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**5 USC 601–612 (chapter 6)**

The Analysis of Regulatory Functions. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**10 USC 2686**

Utilities and Services: Sale; Expansion and Extension of Systems and Facilities. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**15 USC Chapter 96 (P.L. 106–229)**

Electronic Signatures in Global and National Commerce Act (also known as the “E–Sign Act”). (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**17 USC 101, 501**

Copyrights. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**18 USC 701**

Official Badges, Identification Cards, Other Insignia. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**29 USC 762 (P.L. 101–336)**

Americans with Disabilities Act of 1990. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**29 USC 794d (P.L. 99–506)**

Rehabilitation Act of 1975. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**31 USC 1115, 1116 (P.L. 103–62)**

The Government Performance and Results Act (GPRA). (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**40 USC 759 (P.L. 100–235)**

Computer Security Act of 1987. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**40 USC 762 (P.L. 100–542)**

Telecommunications Accessibility Enhancement Act of 1988. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**41 USC 413 (P.L. 103–355)**

Tests of Innovative Procurement Methods and Procedures (The Federal Acquisition Streamlining Act of 1994 (FASA)). (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**44 USC 3101–3107 (Chapter 31)**

Records Management by Federal Agencies. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**44 USC, Chapter 35**

Coordination of Federal Information Policy (Paperwork Reduction Act of 1995 and The Federal Information Security Management Act). (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**44 USC Chapters 29, 31, and 33 (P.L. 94–575)**

Federal Records Management Amendments of 1976. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**44 USC 3501–3520 (P.L. 96–511)**

Paperwork Reduction Act of 1980. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**47 USC 151, 157, 158, 201, 203, 552, 553, 571–73 (P.L. 104–104)**

Telecommunications Act of 1996. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**47 USC 226 (P.L. 101-435)**

Telephone Operator Consumer Service Improvement Act. (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

**RCS DD-PA (AR)-1381**

Visual Information Production Request and Report

**RCS CSIM-46**

Information Management Requirement/Project Document

**RCS CSIM-59**

VI Annual Workload and Cost Data Report

**Section III****Prescribed Forms**

Except where otherwise indicated below, the following forms are available as follows: DA forms are available on the Army Electronic Library (AEL) CD-ROM (EM 0001) and the APD Web site (<http://www.apd.army.mil>); DD forms are available from the OSD Web site (<http://www.dior.whs.mil>); and SF forms are available from the GSA Web site (<http://www.gsa.gov>).

**DA Form 4103**

Visual Information Product Loan Order. (Prescribed in para 7-4g.)

**DA Form 5695**

Information Management Requirement/Project Document. (Prescribed in para 7-7c(1).)

**DA Form 5697**

Army Visual Information Activity Authorization Record. (Prescribed in para 7-4c.)

**DD Form 1367**

Commercial Communications Work Order (Prescribed in para 6-4c(2).)

**DD Form 1995**

Visual Information (VI) Production Request and Report. (Prescribed in para 7-8a(6).)

**DD Form 2537**

Visual Information Caption Sheet. (Prescribed in para 7-10b.)

**SF 258**

Agreement to Transfer Records to the National Archives of the United States (Prescribed in para 8-5f.)

**Section IV****Referenced Forms****DA Form 11-2-R**

Management Control Evaluation Certification Statement

**DD Form 1391**

FY \_\_\_\_ Military Construction Project Data

**Appendix B****Telecommunications Services Authorized for Specific Activities****B-1. Army National Guard (ARNG)**

Installation voice and data services may be provided to off-post ARNG units, activities, and detachments on a reimbursable basis with funding from the ARNG. On-post voice and data services to ARNG units, activities, and detachments will be provided as common BASOPS services with funding provided per the current Army reimbursement policy for BASOPS services. (See ASA(FM&C)Web site: <http://www.asafm.army.mil/pubs/pubs.asp>.)

## **B-2. United States Army Reserve (USAR)**

Installation voice and data services may be provided to on-post and off-post Army Reserve units and activities on a reimbursable basis with funding from the USAR. On-post voice and data services to USAR units and activities will be provided as common BASOPS services with funding provided in accordance with the current Army reimbursement policy for BASOPS services. (See ASA(FM&C) Web site: <http://www.asafm.army.mil/pubs/pubs.asp>.)

## **B-3. Reserve Officer Training Corps (ROTC)**

Local voice and data services for senior and junior ROTC detachments are normally provided by the supported educational institution. Services beyond those provided by the educational institution may be provided by the supporting DOIM on a reimbursable basis. The requesting ROTC detachments are responsible for ensuring that funding is available through their chain of command. All available services, including FTS and equivalent service, should be considered prior to approving commercial service.

## **B-4. Army MWR programs and NAF activities**

The Army policy for providing telecommunications services to Army MWR operations is defined within AR 215-1. Class A-2 official telephone service will be provided in CONUS and OCONUS on a nonreimbursable basis for the conduct of executive control and essential command supervision (ECECS) and C2/management functions. This service provides Army MWR the capability to execute the Army's fiscal and fiduciary responsibility to manage the NAF Government assets from point of receipt to final disposition. Access to data networks or cable plants will be provided per paragraph 6-4 on an as-needed basis. Access to other data services may be provided if the capacity exists and it does not inhibit Army C2 functions. If the existing telecommunications and network systems do not have the capacity to allow MWR traffic, RCIOs and DOIMs will include it in future system upgrades.

a. All MWR directly operated activities will be provided Class A-2 telephone service and data transfer services, such as administrative, sales, and service within the confines of this paragraph.

b. MWR commercial contracted concessions will use commercial telephone service. Class B service and access to installation data services may be provided if commercial service is not available.

## **B-5. Defense Commissary Agency (DeCA)**

Official common user telephone and data services are authorized for use by commissary store activities when essential to commissary management. Management functions include statistical data gathering and reporting, personnel management, official telecommunications with other Army installations and Government agencies, and procuring contractual services.

a. Class A-3 and C telephone service is provided CONUS commissary officers, their assistants, and administrative control sections.

b. Class A-4 telephone service is authorized for use by cashiers for the purpose of official telecommunications with the local banking facilities for check collection.

c. Class A-4 telephone service is installed in locations where only cashier personnel have access to the service.

d. Class-C telephone service is authorized for managers of meat departments, produce departments, grocery departments, warehouses, and associated commissary annexes. This service is provided on a reimbursable basis only in the office of the department warehouse and annex managers.

e. At installations where the commissary officer is not authorized to contract for voice and data service, the DOIM may provide support for the requirement. In such cases, a host/tenant agreement is executed. Depending on the source of reimbursement, this agreement may be between the DOIM and the commissary officer or the area commissary field director.

f. Official common user communications services are authorized on a nonreimbursable basis for use by commissary stores overseas, including Alaska, Puerto Rico, and Hawaii.

g. If the existing telecommunications and network systems do not have the capacity or would otherwise be adversely impacted by DeCA traffic, MACOMs and DOIMs will plan to accommodate such traffic in future system upgrades or otherwise provide right-of-way access and support for the separate acquisition of commercial voice and data telecommunications services for DeCA facilities.

## **B-6. Army and Air Force Exchange Services (AAFES)**

AAFES HQ, exchange regions, area exchanges, exchange managers, main store managers, and military clothing sales store operations will be authorized Class A-2 official telephone service in CONUS and OCONUS on a nonreimbursable basis for official business (that is, command management functions). Access to commercial circuits for the conduct of AAFES business will be on a reimbursable basis at Government rates whenever possible. Access to data services, networks, or cable plant will be provided by the installation to accomplish command management functions that require data transfer. These services are on an as-needed basis, provided the capacity exists and it does not inhibit Army C2 functions. All AAFES directly operated activities are authorized Class C telephone service and data transfer

services, such as administrative, sales, and service within the confines of this paragraph. AAFES commercial contracted concessions will use commercial telephone service. Class B service and access to installation data services may be provided if commercial service is not available.

#### **B-7. Contractors**

*a.* Contractors providing resale services related to NAFI operations will use commercial telephone service when available. Class B service may be provided if commercial service is not available. Contractors normally will be provided only proximity access to intra-post class C service necessary for coordinating local support and for fire and safety reasons. Contractors normally will not be provided access to data services and networks for the conduct of official business unless stipulated as a provision of their contract.

*b.* Contractors providing APF type support may receive official telephone service. The contracting officer determines if such service is advantageous to the Government and is mission essential. Authorized service must be specified in the contract as Government furnished.

*c.* When official telephone service is authorized, Class A and/or Class C service may be provided, as determined by the DOIM, contracting officer, or contracting officer's representative for specific contracts. DOIMs will charge the contractor public tariff rates for supplemental services. These services include facilities such as key equipment, special switchboards, private lines, and FX lines for the exclusive use of the contractor. In the absence of tariff rates, or excessive rates, the installation commander determines equitable charges based on the actual cost of providing the services.

*d.* When the Army furnishes long-distance service from Class B-2 telephones to contractors on a reimbursable basis, the contractor will pay all actual charges and all taxes. Army activities do not provide official Government telephone calling cards to contractors. The procedures for authorizing, controlling, and recording long-distance service also apply to official collect telephone calls that contractor personnel place or receive.

*e.* The agency funding the contract reimburses the host installation for telephone charges that the contractor incurs. CJCSI 6215.01B provides guidance on when U.S. civilian contractor personnel can use the DSN.

#### **B-8. Field operating activities/direct reporting units**

FOAs and DRUs located on an Army installation, or stationed nearby with agreement, may be provided the following telephone services:

*a.* Class A-1 service, when performing a military function, to include medical.

*b.* Class A-2 service, when performing a civil works function.

*c.* A mix of Class A-1 and A-2 service when performing both a military and a civil works function. The mix of service type is mutually determined at the local level.

*d.* Access to data services and networks are provided when the capacity exists and it does not inhibit Army C2 functions already on the network.

#### **B-9. Department of Defense Dependent Schools**

Provide Class A-2 and Class C telephone service to Government-operated school facilities for military dependents on an Army installation. Access to other voice and data services is dependent upon local agreements.

#### **B-10. American Red Cross (ARC)**

Provide official voice and data service without reimbursement if ARC personnel supplement MWR functions. The ARC must use separate, unofficial voice and data service to conduct unofficial business.

#### **B-11. Army lodging TDY facilities**

The Comptroller General has ruled, "Where sufficient official need exists for a telephone not in private quarters, appropriated funds may be used, regardless of the incidental personal benefit to the occupant." (See also DODI 1015.12, enclosure 4). Therefore, the following guidelines are provided for official telephone service in Army transient facilities. RCIOs/DOIMs will—

*a.* Set controls to ensure that the Army does not pay for unofficial or personal toll calls with appropriated funds, establish controls through system hardware and software configurations, if possible, and set up direct toll billing procedures for transient residents.

*b.* Authorize direct access when necessary, from transient billets to DSN and the local calling area. Appropriated funds must not be used to pay message unit charges accrued for unofficial or personal individual calls to the local area.

*c.* Implement the requirements detailed in the Telephone Operator Consumer Service Improvement Act (P.L. 101-435, codified in 47 USC 226).

#### **B-12. Official telephone service for hospitalized active duty military personnel**

A hospital room is the duty location for hospitalized personnel. If capacity exists in the installation telephone

infrastructure, provide Class C telephone service. The installation DOIM has authority to approve a higher class of service or special features.

### **B-13. Private telephone service for hospital patients**

The hospital administrator will coordinate with the installation DOIM for infrastructure for the local telephone company to provide private unofficial telephone service to hospital patients upon request. A contractual agreement for commercial service is solely between the patient and the commercial company providing the service. Local telephone companies will reimburse the installation DOIM for any infrastructure used to support private unofficial telephone service to patients. When the Government provides Class B service, the patient must pay the recurring cost plus the cost of individual toll calls.

### **B-14. Nonprofit organizations**

The commander or appropriate DA civilian supervisor who is the head of an organization within an Army component, may authorize support to certain nonprofit organizations in a manner consistent with the provisions of DOD 5500.7-R. Nonprofit organizations do not pay service charges for Class A or C telephone service on an Army installation when performing a function related to, or furthering, a Federal Government objective or one that is in the interest of public health and welfare. Nonprofit organizations will reimburse the installation for all long-distance telephone services. DSN access will not be authorized. Access to data services and networks may be furnished provided the capacity exists and it does not reduce the effectiveness of security or operational functions of the network. The extent of services will be based upon local agreements.

### **B-15. Government employee labor unions**

Class B-2 rates for telephone service apply. Only reimbursable long-distance telephone services may be provided. Labor unions are not authorized DSN access. Access to other voice and data services is dependent upon local agreements.

### **B-16. Public schools**

Public schools normally use commercial voice and data service on Army installations. If commercial service is unavailable, the school reimburses the Government for the cost of Class B services. Access to data services and networks may be furnished provided the capacity exists and it does not reduce the effectiveness of security or operational functions of the network. The extent of services will be based upon local agreements.

### **B-17. Civilian post offices on military installations**

Provide reimbursable voice and data service to on-base civilian post offices, branches, or stations when requested. The extent of services is dependent upon local agreements.

### **B-18. Soldiers in the barracks**

All private telephone service for soldiers in the barracks will be through the AAFES contract. Other organizations are not authorized to establish telephone service for soldiers in the barracks. Access to other voice and data services is dependent upon local agreements.

### **B-19. Army Community Service (ACS) Volunteers and Army family support groups**

ACS volunteers and Army family support groups are authorized to place calls or use e-mail using official Government communications networks (for example, DSN and FTS) through local operations centers or installation telephone operators as long as such communications support the APF command support functions. Access to data services and networks may be furnished provided the capacity exists and does not reduce the effectiveness of security or operational functions of the network. The extent of services will be based upon local agreements.

## **Appendix C**

### **Management Control Evaluation Checklist**

#### **C-1. Function**

The functions covered by this checklist are the administration of Army information management (IM) and information technology (IT). They include key controls for CIO management, IT Architecture, information assurance, C4/IT support and services, visual information management, records management, and publishing management.

#### **C-2. Purpose**

The purpose of this checklist is to assist HQDA, FOAs, MACOMs, and installations in evaluating the key management controls outlined below; it is not intended to cover all controls.

### C-3. Instructions

Answers must be based on the actual testing of management controls (such as document analysis, direct observation, sampling, simulation). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2-R (Management Control Evaluation Certification Statement).

### C-4. Test questions

*a. Responsibilities (chap 2).* Have C4/IT plans, programs, and requirements been coordinated with the appropriate IA managers? (All)

*b. CIO management (chap 3).*

(1) Are the duties and responsibilities of the senior information manager clearly designated in the organization's mission and function? (HQDA, region, MACOM, FOA)

(2) Has the installation clearly established a region CIO who has the sole responsibility of implementing the region's IM/IT program?

(3) Has the organization analyzed (and documented the analysis of) its mission and revised mission-related and administrative work processes, as appropriate, before making significant IT investments in support of those processes? (HQDA, MACOM, FOA)

(4) Does the organization have a strategic plan that is linked to their mission? Is it periodically updated? (HQDA, MACOM, FOA)

(5) Has a forum been established to develop and implement C4/IT procedures, requirements, and priorities? (RCIO/MACOM/DOIM)

(6) Does the organization have a clearly defined process for submitting and screening new IT investment proposals for management consideration? (MACOM, region, FOA)

(7) Does the IT investment screening process include addressing the following questions and resolving all issues prior to making an IT investment and initiating any process analysis or improvement? (HQDA, MACOM, region, FOA)

(8) Does the process support core/priority mission functions? (HQDA, MACOM, region, FOA)

(9) Can the process be eliminated? (HQDA, MACOM, FOA)

(10) Can the process be accomplished more effectively, efficiently, and at less cost by another Government source (for example, another MACOM or Federal organization) or the private sector?

(11) Does the IT investment process clearly establish who in the organization has the responsibility and authority for making final IT-related investment decisions? (HQDA, MACOM, FOA)

(12) Are exceptions to the IT investment-screening process clearly documented? (HQDA, MACOM, FOA)

(13) Does the organization require that management evaluations for the IT investment screening process, as well as scoring, ranking, and prioritization results, be documented (either manually or through the use of automated applications such as a decision support tool)? (HQDA, MACOM, FOA)

(14) Are IT investment decisions made a part of the organization's integrated capital planning process or are IT projects separated out? (HQDA, MACOM, FOA)

(15) Does the organization have a process in place to conduct periodic reviews (in-house or via outside consultant/expert) of its current IT investment portfolio to assess alignment with mission needs, priorities, strategic direction, or major process reengineering? (HQDA, MACOM, FOA)

(16) Does the organization have a process for documenting and disseminating results of this review? (HQDA, MACOM, FOA)

(17) Are process analysis and improvements for warfighter processes documented in the initial capabilities document using the DOTMLPF requirements methodology as defined by the Army requirements generation process in AR 71-9? (HQDA, MACOM, FOA)

(18) Have webification status and future webification plans been reported within the AITR? (All)

(19) Have functional managers developed a set of goals and objectives with performance measures to gauge overall functional mission improvement? Have accomplishments been reported to enterprise-level managers? (All)

(20) Have performance measures been developed for each IT investment that supports organizational mission before execution of that investment? (HQDA, MACOM, FOA, PEO, PM)

(21) Have IT investments been synchronized to overall DOD/Army mission priorities? (HQDA, MACOM, PEO, PM)

(22) Are performance measures linked to management-level goals, objectives, and measures? (All)

(23) Are requirements being developed in consonance with the Army's goal of creating an end-state strategy of implementing an ERP business solution throughout a fully integrated Army logistics environment? (HQDA, MACOM)

*c. Army Enterprise Architecture (chap 4).* (All.)



- (1) Has the organization developed the appropriate architectures for the AKEA that support the DOTMLPF components as mapped to the Net-Centric Operations and Warfare Reference Model?
- (2) Has the organization developed the appropriate architectures for the Battle Command Architecture that support Joint Capabilities and Integrated Development System (JCIDS), acquisition of SoS and FoS, software blocking, force development, and lessons learned from operations?
- (3) Has the organization developed the appropriate architectures for the ABEA that support the migration of current systems infrastructure, net-centric warfare, enterprise application integration, and business process modernization and align with the seven DOD BEA domains: Acquisition/Procurement, Human Resource Management, Finance and Accounting, Logistics, Technical Infrastructure, Installations and Environment, and Strategic Planning and Budgeting?
- d. Information assurance (chap 5) (Applies to MACOM, separate reporting activity, region, installation, unit.)*
  - (1) Has an IA program been established at all levels?
  - (2) At each level, have the appropriate IA personnel been appointed?
  - (3) Are IAVA messages being acted upon and reported in a timely fashion?
  - (4) Are all information systems and networks accredited and certified? When a new information system is created, does it meet all accreditation and certification standards?
  - (5) Have the appropriate software controls been implemented to protect system software from compromise, subversion, and/or tampering?
  - (6) Is only approved software being used on Army networks and stand-alone workstations?
  - (7) Are database management systems that contain classified defense information protected to the highest security classification of any identifiable database element?
  - (8) Are developers of Army systems that include software using appropriate security features in the initial concept exploration phase of the life-cycle system development model? Is the software being independently tested and verified prior to release for operation?
  - (9) Are developers of Army systems employing IA and security requirements in the design, development, and acquisition of the system, software, and/or physical environment of the system?
  - (10) Have all personnel received the level of training necessary and appropriate to perform their designated information assurance responsibilities?
  - (11) Are proper password control and procedures being implemented within commands? Are minimum requirements of accountability, access control, least privilege, and data integrity being met?
  - (12) Are appropriate measures to secure all communications devices to the level of security classification of the information to be transmitted over such communication equipment being met?
  - (13) Has an effective risk management program been established by the commander? Has a periodic review of the risk management program taken place in the recent past?
  - (14) Is the IA manager NTSSI 4011 certified?
- e. C4/IT support and services (chap 6).*
  - (1) Is a process in place for acquiring IT and ensuring all required licensing and registration are accomplished? (DOIM)
  - (2) Is the DOIM the single organization responsible for the oversight and management of installation IT? (DOIM)
  - (3) Are periodic reviews being conducted of current IT to ensure they are still required and meeting user needs? (HQDA, MACOM)
  - (4) Are quarterly reviews being conducted of current IT within the AITR and verified by the users that they are still required and meeting users needs? (HQDA, MACOM)
  - (5) Are evaluations being conducted of existing systems for obsolescence? (HQDA, MACOM)
  - (6) Is an accurate inventory being maintained and validated annually for IT equipment? (DOIM, IMO)
  - (7) Are continuity of operations plans and procedures documented, distributed, and tested at least biannually? (MACOM, DOIM)
  - (8) Has guidance been provided to ensure all software is checked for viruses before being loaded? (DOIM)
  - (9) Are existing capabilities and/or assets considered prior to upgrading, improving, or implementing local area networks? (RCIO, DOIM)
  - (10) Are uneconomical IT service contracts identified and terminated? (All)
  - (11) Has the DOIM coordinated the acquisition of licenses with the ASCPO prior to entering into an agreement with a COTS vendor? (DOIM)
  - (12) Are spare capacity and functional expansion on IT being considered and/or used when new requirements are identified? (All)
  - (13) Has the DOIM reported its server consolidation status for all its Army tenants to the Army CIO/G-6? (DOIM)
  - (14) Are measures being taken to ensure that hard drives are disposed of properly? (DOIM)
  - (15) Are criteria established for justifying and approving the acquisition of cellular phones and pagers? (RCIO, DOIM)

(16) Has guidance been provided to review and revalidate cellular telephones and pagers every 2 years? (RCIO, DOIM)

(17) Do procedures require the establishment of a reutilization program to identify and turn in cellular phones and pagers that are no longer required or seldom used? (DOIM)

(18) Is there a requirement for cellular phones and pagers to be recorded in the property book? (DOIM)

(19) Has the DOIM implemented accountable billing procedures? (DOIM)

(20) Have maintenance and support strategies been devised to minimize overall systems life-cycle cost at an acceptable level of risk? (PEO, PM, MACOM)

(21) Do safeguards exist to ensure that computer users do not acquire, reproduce, or transmit software in violation of applicable copyright laws? (RCIO, DOIM, IMO)

(22) Are private sector service providers made aware that written assurance of compliance with software copyright laws may be required? (RCIO, DOIM, IMO)

(23) Are existing portals being migrated to AKO and AKO-S? (All)

(24) Does each Web site contain a clearly defined purpose statement that supports the mission of the organization? (All)

(25) Are users of each publicly accessible Web site provided with privacy and security notice prominently displayed or announced on at least the first page of all major sections of each Web information service? (All)

(26) If applicable, does this Web site contain a disclaimer for external links notice for any site outside of the official DOD Web information service (usually the .mil domain)? (All)

(27) Is this Web site free of commercial sponsorship and advertising? (All)

(28) Is the Web site free of persistent cookies or other devices designed to collect personally identifiable information about Web visitors? (All)

(29) Is each Web site made accessible to handicapped users in accordance with Section 508 of the Rehabilitation Act? (All)

(30) Is operational information identified below purged from publicly accessible Web sites? (All)

(a) Plans or lessons learned that would reveal military operations, exercises, or vulnerabilities.

(b) Sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program.

(c) Personal information about U.S. citizens, DOD employees, and military personnel, to include the following:

— Social security account numbers.

— Dates of birth.

— Home addresses.

— Directories containing name, duty assignment, and home telephone numbers.

— Names, locations, or any other identifying information about family members of DOD employees or military personnel.

(d) Technological data such as—

— Weapon schematics.

— Weapon system vulnerabilities.

— Electronic wire diagrams.

— Frequency spectrum data.

(31) Are operational security tip-off indicators in the following categories purged from the organization's publicly accessible Web site? (All)

(a) *Administrative.*

— Personnel travel (personal and official business).

— Attendance at planning conferences.

— Commercial support contracts.

— FOUO.

(b) *Operations, plans, and training.*

— Operational orders and plans.

— Mission-specific training.

— Exercise and simulations activity.

— Exercise, deployment or training schedules.

— Unit relocation/deployment.

- Inspection results, findings, deficiencies.
- Unit vulnerabilities or weaknesses.

*(c) Communications.*

- Spectrum emissions and associated documentation.
- Changes in activity or communications patterns.
- Use of Internet and/or e-mail by unit personnel (personal or official business).
- Availability of secure communications.
- Hypertext links with other agencies or units.
- Family support plans.
- Bulletin board/messages between soldiers and family members.

*(d) Logistics/maintenance.*

- Supply and equipment orders/deliveries.
- Transportation plans.
- Mapping, imagery, and special documentation support.
- Maintenance and logistics requirements.
- Receipt or installation of special equipment.

(32) Has the Web site reviewer performed a key word search for any of the following documents and subsequently removed sensitive personal or unit information from publicly accessible Web sites? (All)

- Deployment schedules.
- Duty rosters
- Exercise plans.
- Contingency plans.
- Training schedules.
- Inspection results, findings, deficiencies.
- Biographies.
- Family support activities.
- Phone directories.
- Lists of personnel.

(33) Are existing infostructure capabilities and assets considered prior to upgrading, improving, or modernizing? (HQDA, MACOM)

(34) Is the fully qualified domain name (for example, <http://www.us.army.mil> or <http://apd.army.mil>) for Army sites registered with the GILS at <http://sites.defenselink.mil/>, and the contact information updated annually?

(35) Are the Web servers IAVA compliant and placed behind a reverse proxy server?

*f. Visual information (chap 7).*

(1) Does the mission guidance include responsibilities of the VI manager, to include organization structure and responsibilities of all components of the organization, and does it state that this VI manager provides overall policy, plans, and standards for all VI operations? (RCIO)

(2) Is the VI manager the single staff manager for all VI functions on the installation? (RCIO)

(3) Are all VI services and equipment, except those specifically exempted by the RCIO, consolidated for centralized VI management? (RCIO)

(4) Do all VI activities under the RCIO's purview have a Defense Visual Information Authorization Number (DVIAN)? (RCIO)

(5) Does the VI manager approve all VI equipment required by AR 25-1, chapter 7? (RCIO)

(6) Is VI policy being followed for multimedia/VI productions? (For example, DD Form 1995 is used, funds identified up front, PAN registers maintained, DAVIS searches conducted, service support contracts awarded for less than 50 percent of the total production cost, Nonlocal DAVIS entries, using JVIS contracting facility (RCIO and installation).)

(7) Is a production folder maintained for the life cycle of local productions? (FOA and installation)

(8) Has your VI activity developed and implemented a standard level of agreement document to include an SOP? (RCIO and installation)

*g. Records management (chap 8).*

(1) Is a records management program established in your organization? (All)

- (2) Has a records official been appointed to manage the internal records of the organization and its subelements?
  - (3) Are records managers included in the planning process for new or replacement automated systems? (All)
  - (4) Are records management reviews of agency and commands conducted at least once every 3 years? (All)
  - (5) Have instructions been issued specifying the degree of protection to be afforded records stored and used electronically in accordance with classification, releasability, Freedom of Information Act, and Privacy Act? (All)
  - (6) Are procedures in place to ensure software and equipment are available to read electronic records throughout their retention period? (All)
  - (7) Do all information collections from the public, affecting 10 or more individuals have OMB approval? (All)
  - (8) Do the documents have special management or archiving requirements?
- h. Publishing and printing management (chap 9).*
- (1) Are policy publications issued as regulations? (HQDA)
  - (2) Are higher-echelon forms used in lieu of creating local forms for the same purpose? (All)
  - (3) Is a program established to encourage the design and use of electronically generated forms? (HQDA)
  - (4) Are Army-wide forms for electronic generation approved by the functional proponent and APD? (HQDA)
  - (5) Is field printing coordinated through DAPS and the printing officer? (All)

### **C-5. Supersession**

This checklist replaces the checklist for the administration of Army IM and IT previously published in AR 25-1, dated 31 May 2002.

### **C-6. Comments**

Help make this a better tool for evaluating management controls. Submit comments to CIO/G-6, ATTN: SAIS-EIG, 107 Army Pentagon, Washington, DC 20310-0107.

## **Glossary**

### **Section I Abbreviations**

#### **AAE**

Army Acquisition Executive

#### **AAFES**

Army and Air Force Exchange Service

#### **AASA**

Administrative Assistant to the Secretary of the Army

#### **ABCA**

American, British, Canadian, Australian

#### **ABEA**

Army Business Enterprise Architecture

#### **ABIC**

Army Business Initiative Council

#### **ACAT**

acquisition category

#### **ACERT**

Army Computer Response Team

#### **ACP**

Allied Communications publication

#### **ADS**

authoritative data source

#### **AEI**

Army Enterprise Infostructure

#### **AEL**

Army Electronic Library

#### **AFIP**

Armed Forces Institute of Pathology

#### **AFRTS**

Armed Forces Radio and Television Service

#### **AITR**

Army Information Technology Registry

#### **AEA**

Army Enterprise Architecture

#### **AKEA**

Army Knowledge Enterprise Architecture

#### **AKM**

Army Knowledge Management

#### **AKO**

Army Knowledge Online

**AMC**

U.S. Army Materiel Command

**AMP**

Army Modernization Plan

**ANCDMP**

Army Net-Centric Data Management Program

**ANSI**

American National Standards Institute

**APD**

Army Publishing Directorate

**APF**

appropriated fund(s)

**APP**

Army Publishing Program

**AR**

Army Regulation

**ARC**

American Red Cross

**ARIMS (formerly MARKS)**

Army Records Information Management System

**ARNG**

Army National Guard

**ARSTAF**

Army Staff

**ASA(ALT)**

Assistant Secretary of the Army (Acquisition, Logistics and Technology)

**ASA(FM&C)**

Assistant Secretary of the Army (Financial Management & Comptroller)

**ASC**

Army Signal Command

**ASCPO**

Army Small Computer Program Office

**ASD**

Assistant Secretary of Defense

**AVID**

Army Visual Information Directorate

**AWRAC**

Army Web Risk Assessment Cell

**BASECOM**

base communications

**BASOPS**

base operations

**BOD**

beneficial occupancy date

**BPA**

blanket purchase agreement

**BPR**

Business process re-engineering

**C2**

command and control

**C3**

command, control, communications

**C3I**

command, control, communications, and intelligence

**C4**

command, control, communications, and computers

**C4I**

command, control, communications, computers and intelligence

**C4ISR**

command, control, communications, computers, intelligence, surveillance, and reconnaissance

**C4/IT**

command, control, communications, computers and information technology

**CAC**

Common Access Card

**CALS**

Continuous Acquisition and Lifestyle Support

**CAP**

Component Accessioning Point

**CATV**

cable television

**CCB**

Configuration Control Board

**CCS2**

command, control, and subordinate systems

**CCTV**

closed circuit television

**CDAd**

Component Data Administrator

**CD-ROM**

Compact Disk-Read Only Memory

**CECOM**

U.S. Army Communications-Electronics Command

**CFR**

Code of Federal Regulations

**CIK**

Crypto Ignition Key

**CIO**

Chief Information Officer

**CJCS**

Chairman, Joint Chief of Staff

**CJCSI**

Chairman, Joint Chief of Staff instruction

**CMO**

Collaboration Management Office

**COIs**

communities of interest

**COIDAds**

communities of interest data administrators

**COMCAM**

combat camera

**COMSEC**

communications security

**CONUS**

continental United States

**COOP**

continuity of operations plan

**CoP**

community of practice

**COTS**

commercial off-the-shelf

**CPIM**

Capital Planning and Investment Management

**CSA**

Chief of Staff, Army

**CSTS**

commercial satellite television services

**CTA**

common table of allowances

**CTSF**

Central Technical Support Facility



**DA**

Department of the Army

**DAA**

designated approval authority

**DAB**

Defense Acquisition Board

**DAPS**

Defense Automated Printing Service

**DAMVIPDP**

Department of the Army Multimedia/Visual Information Production and Distribution Program

**DAVIS**

Defense Automated Visual Information System

**DBMS**

database management systems

**DCS**

Deputy Chief of Staff

**DCID**

Director of Central Intelligence Directive

**DeCA**

Defense Commissary Agency

**DISA**

Defense Information Systems Agency

**DISAC**

Defense Information Systems Agency circular

**DISN**

Defense Information Systems Network

**DITIS**

Defense Instructional Technology Information System

**DITSCAP**

Defense IT Security Certification and Accreditation Process

**DLA**

Defense Logistics Agency

**DMRD**

Defense Management Resource Decision

**DMS**

Defense Message System

**DOD**

Department of Defense

**DODAF**

Department of Defense Architecture Framework

**DODD**

Department of Defense directive

**DODI**

Department of Defense instruction

**DOIM**

director of information management

**DOTMLPF**

doctrine, organization, training, materiel, leadership, personnel, and/or facilities

**DPP**

data performance plan

**DPPS**

data performance plan system

**DRMS**

Defense Reutilization and Marketing System

**DRU**

direct reporting unit

**DSAWG**

DISN Security Accreditation Working Group

**DSN**

Defense Switched Networks

**DTS**

Defense Telephone System

**DTS-W**

Defense Telecommunications Service-Washington

**DVD**

digital video disk

**DVI**

Defense Visual Information

**DVIAN**

Department of Defense Visual Information Activity Number

**DVIC**

Defense Visual Information Center

**e-Army**

Electronic Army

**e-mail**

electronic mail

**EB/EG**

electronic business/electronic government

**ECECS**

executive control and essential command supervision

**EID**

enterprise identifier

**EIPP**

Educational Institution Partnership Program

**ELA**

enterprise license agreement

**EO**

Executive order

**ERP**

enterprise resource planning

**ESA**

enterprise software agreement

**ESI**

Enterprise Software Initiative

**ESM**

Enterprise Systems Management

**FAR**

Federal Acquisition Regulation

**FOA**

field operating agency

**FOIA**

Freedom of Information Act

**FORSCOM**

U.S. Army Forces Command

**FoS**

Family-of-Systems

**FOUO**

For Official Use Only

**FTS**

Federal Telecommunications System

**FX**

Foreign Exchange

**FY**

fiscal year

**GBS**

Global Broadcast Service

**GETS**

Government Emergency Telecommunication Service

**GIG**

Global Information Grid

**GILS**

Government Information Locator Service

**GOTS**

Government off-the-shelf

**GPO**

Government Printing Office

**GPS**

global positioning system

**GSA**

General Services Administration

**HMW**

health, morale, and welfare

**HQ**

headquarters

**HQDA**

Headquarters, Department of the Army

**HQIM**

HQDA Information Manager

**HUMINT**

human intelligence

**IA**

information assurance

**IAIC**

Intra-Army Interoperability Certification

**IAM**

information assurance manager

**IANO**

information assurance network officer

**IAPM**

information assurance program manager

**IASO**

information assurance security officer

**IAVA**

Information Assurance Vulnerability Alert

**IESS**

Information Exchange Standards Specifications

**IM**

information management

**IMA**

Installation Management Agency

**IMI**

interactive multimedia instruction

**IMO**

information management officer

**Inmarsat**

International Maritime Satellite

**INSCOM**

U.S. Army Intelligence and Security Command

**IRM**

Information Resources Management

**ISA**

inter-Service support agreement

**ISP**

Internet service provider

**IT**

information technology

**ITM**

information technology management

**JCCC**

Joint Combat Camera Center

**JCIDS**

Joint Capabilities and Integrated Development System

**JITC**

Joint Interoperability Test Command

**JPO**

Joint Program Office

**JS**

Joint Staff

**JTA**

Joint Technical Architecture (DOD)

**JTA-A**

Joint Technical Architecture-Army

**JVISDA**

Joint Visual Information Services Distribution Activity

**JWICS**

Joint Worldwide Intelligence Communications System

**JWRAC**

Joint Web Risk Assessment Cell

**LAN**

local area network

**LDAP**

Lightweight Directory Access Protocol

**MACOM**

major Army command

**MARS**

Military Affiliate Radio System

**M/CATV**

master/community antenna television

**MCEB**

Military Communications-Electronics Board

**MDEP**

Management Decision Evaluation Package

**MEDCOM**

U.S. Army Medical Command

**MFP**

materiel fielding plan

**MICO**

Management Information Control Office

**MILCON**

military construction

**MILSATCOM**

Military Satellite Communications

**MILSTAR**

Military Strategic and Tactical Relay System

**MSC**

major subordinate command

**MTOE**

modified table of organization and equipment

**MWR**

morale, welfare, and recreation

**NAC**

National Audiovisual Center

**NAF**

nonappropriated fund(s)

**NAFI**

nonappropriated fund instrumentalities

**NARA**

National Archives and Records Administration

**NATO**

North Atlantic Treaty Organization

**NCR**

National Capital Region

**NETCOM**

U.S. Army Network Enterprise Technology Command

**NETOPS**

network operations

**NFIP**

National Foreign Intelligence Program

**NIAP**

National Information Assurance Partnership

**NIPRNET**

Unclassified but Sensitive Internet Protocol Router Network

**NSA**

National Security Agency

**NSS**

National Security Systems

**OA**

Operational Architecture

**O&M**

operation and maintenance

**OCONUS**

outside of the continental United States

**OMB**

Office of Management and Budget

**OPA**

Other Procurement, Army

**ORL**

office record list

**OSA**

Office of the Secretary of the Army

**OSD**

Office of the Secretary of Defense

**OV**

Operational View

**PA**

Public Affairs

**Pam**

Pamphlet

**PAN**

production authorization number

**PBD**

Program Budget Decision

**PAO**

public affairs officer

**PC**

end-user microcomputer (personal computer)

**PDA**

personal digital assistant

**PEG**

program evaluation group

**PEO**

program executive officer

**PIN**

personal/production identification number

**PKI**

Public Key Infrastructure

**PM**

program/project/product manager

**POC**

point of contact

**POM**

program objective memorandum

**PPBE**

Planning, Programming, Budgeting, and Execution

**PPS**

precise positioning service

**PPSS**

postproduction software support

**PSN**

Public Switch Network

**RCIO**

regional Chief Information Officer

**RCS**

requirements control symbol

**RDT&E**

research, development, test, and evaluation

**RFS**

request for service

**RHA**

records holding area



**SA**

Systems Architecture

**SAP**

Special Access Program

**SATCOM**

satellite communications

**SB**

supply bulletin

**SCI**

sensitive compartmented information

**SCIF**

sensitive compartmented information facility

**SECARMY**

Secretary of the Army

**SF**

Standard Form

**SGML**

Standard Generalized Markup Language

**SIPRNET**

Secret Internet Protocol Router Network

**SLA**

service level agreement

**SOP**

standing operating procedure

**SoS**

System-of-Systems

**SRS**

Strategic Readiness System

**SSL**

secure sockets layer

**STARC**

State Area Command

**STE**

secure telephone equipment

**STU-III**

secure telephone unit, type III

**SV**

System View

**TA**

Technical Architecture

**T&E**

test and evaluation

**T-ASA**

Television-Audio Support Activity

**TAP**

The Army Plan

**TDA**

table of distribution and allowances

**TDD**

telecommunication devices for the deaf

**TECHCON**

technical control

**TJAG**

The Judge Advocate General

**TNOSC**

Theater Network Operations and Security Center

**TOE**

table of organization and equipment

**TRADOC**

U.S. Army Training and Doctrine Command

**TV**

Technical View (architecture)

**UFR**

unfunded requirement

**UIC**

unit identification code

**URL**

uniform resource locator

**USAR**

United States Army Reserve

**USARMDA**

U.S. Army Records Management and Declassification Agency

**USC**

United States Code

**VI**

visual information

**VIAMS**

Visual Information Automated Management Software

**VIDOC**

visual information documentation

**VIRIN**

visual information record identification number

**VISP**

Visual Information Systems Program

**VTC**

video teleconferencing

**W3C**

World Wide Web Consortium

**WWW**

World Wide Web

**XML**

eXtensible Markup Language

**XSL/T**

eXtensible Stylesheet Language/Transformation

**Section II****Terms****Access control mechanism**

This permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform.

**Activity**

An Army organization. Within the context of the Army Enterprise Architecture, a specific function that must be performed to produce, consume, or transform information. Activities are grouped into larger processes in support of accomplishing tasks and missions. Depending on the context, an activity or function is performed by an individual, unit, or prime system element.

**Acquisition**

The acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the Federal Government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

**Administrative work processes**

Enabling activities that support mission and mission-related processes and functions (for example, manage legal process, performance assessment, combat health support, family support, and so on).

**Army Net-Centric Data Management Program**

Establishes policy, guidance, and instruction about the set of data standards, business rules, and data models required to govern the definition, production, storage, ownership, and replication of data.

**Application**

Software that performs a specific task or function, such as word processing, creation of spreadsheets, generation of graphics, or facilitating e-mail. An application should be considered a system for the purpose of reporting to the Army Information Technology Registry unless it is part of a larger system already being reported.

**Architecture**

The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time.

**Army Business Enterprise Architecture (ABEA)**

The framework of the business processes and organizations that support the Army's warfighters.

**Army Enterprise Architecture (AEA)**

A disciplined, structured, comprehensive, and integrated methodology and framework that encompasses all Army information requirements, technical standards, and systems descriptions regardless of the information system's use. The AEA transforms operational visions and associated required capabilities of the warfighters into a blueprint for an integrated and interoperable set of information systems that implements horizontal information technology insertion, cutting across the functional stovepipes and Service boundaries. The AEA is the combined total of all the Army's Operational, Technical, and System Architectures.

**Army Knowledge Management**

The Army-wide effort to transform the Army into a net-centric self-learning organization that will improve operational and mission performance.

**Army Recordkeeping Systems Management**

Cost-effective organization of Army files and records contained in any media so that records are readily retrievable; ensures that records are complete, facilitates the selection and retention of permanent records, and accomplishes the prompt disposition of noncurrent records in accordance with National Archives and Records Administration approved schedules.

**Army Visual Information Steering Committee**

A committee chaired by CIO/G-6 that develops recommendations for the CIO/G-6 in regards to Army VI planning, policy, programming, systems, standards, architecture, procedures, organizational structure, combat camera, combat and training development, doctrine, and other related issues.

**Army Web Risk Assessment Cell**

A team of information assurance personnel that conduct ongoing operational security and threat assessments of Army publicly accessible Web sites to ensure compliance with DOD and Army policy and best practices.

**Attribute**

A property or characteristic of one or more entities (for example, race, weight, age). Also, a property inherent in an entity or associated with that entity for database purposes.

**Authentication**

A security service that verifies an individual's eligibility to receive specific categories of information.

**Authoritative data source (ADS)**

An ADS is a data structure and value domain set that is readily available to provide common domains of data values to different databases.

**Automation**

Conversion of a procedure, process, or equipment to automatic operation. When allied to telecommunications facilities, automation may include the conversion to automatic operation of the message processing at an exchange or remote terminal.

**Bandwidth**

The maximum rate at which an amount of data can be sent through a given transmission channel.

**Base case system**

A system that has been fielded and certified through the intra-Army interoperability process.

**Benchmark**

A procedure, problem or test that can be used to compare systems, components, processes, and so forth to each other or to a standard.

**Beneficial occupancy date (BOD)**

Construction complete, user move-in dates.

**Broadcast**

The transmission of radio, television, and data signals through the air waves or fiber optic cable.

**Business/functional process improvement**

A systematic, disciplined improvement approach that critically examines, rethinks, and redesigns mission-delivery processes in order to achieve improvements in performance in areas important to customers and stakeholders (GAO BPR Assessment Guide, 1997). (See also DODD 8000.1.)

**Business process re-engineering (BPR)**

The fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance such as cost, quality, service, and speed. Re-engineering is only part of what is necessary in the radical change of processes; it refers specifically to the design of a new process (DODD 8000.1.)

**Cable television (CATV) system**

A facility consisting of a set of closed transmission paths and associated signal generation, reception, and control equipment that is designated to provide cable service that includes both audio and video programming and that is provided to multiple subscribers.

**Capability**

In the context of the AEA framework, a capability satisfies a requirement, specifically an IT requirement. For example, an Army headquarters element has the requirement to know the location of all friendly and enemy units in its area of operations; situational awareness is the capability that satisfies that requirement.

**Capital Planning and Investment Management (CPIM)**

The CPIM process is to develop C4/IT investment policy and strategic direction that informs Army leaders and directly impacts their POM decisions on all C4/IT expenditures across all functional domains. The CPIM process is collaborative among C4/IT stakeholders, with a focus on C4/IT across the Army (to include all functional domains) throughout the life cycle of IT expenditures and the management of IT assets.

**Class A (official) telephone service**

Telephone service authorized for the transaction of official business of the Government on DOD/military installations; requires access to commercial telephone company central office and toll trunks for the proper conduct of official business.

**Class B (unofficial) telephone service**

Telephone service installed on or in the immediate vicinity of a DOD/military installation served through a military PBX or CENTREX system through which the conduct of personal or unofficial business is authorized. This telephone service has access to commercial telephone company central office and toll trunks.

**Class C (official-restricted) telephone service**

Telephone service authorized for the transaction of official business of the Government on a DOD/military installation and without access to Telephone Company central office or toll trunks.

**Class D (official-special) telephone service**

Telephone service installed on military installations for official business of the Government and restricted to special classes of service, such as fire alarm, guard alarm, and crash alarm.

**Closed circuit television (CCTV)**

Point-to-point signal transmission by cable or directional radiation where the audience is limited by physical control or nonstandard transmission.

**Command and control**

Exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. These functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures that are employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

**Command and control system**

Any system of facilities, equipment (including hardware, firmware, and software), communications, procedures, and

personnel available to commanders at all echelons and in all environments that is essential to plan, direct, and control operations conducted by assigned resources.

**Command, control, and subordinate systems (CCS2)**

Part of the Army command and control system, which encompass all intrinsic subsystems of the five battlefield functional areas at corps and below, representing the battlefield command and control architecture.

**Command, control, communications, and intelligence (C3I)**

One of the four domains used to manage Architecture configurations in the ASA. It includes all systems involved in command, control, and communications (C3) and intelligence.

**Command, control, communications and computer (C4) systems**

Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations.

**Communications**

See *telecommunications*.

**Communications network**

A set of products, concepts, and services that enables the connection of computer systems for the purpose of transmitting data and other forms (for example, voice and video) among the systems.

**Communications security (COMSEC)**

Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

**Communications systems**

A set of assets (transmission media, switching nodes, interfaces, and control devices) that establishes linkage between users and devices.

**Communities of interest (COIs)**

The inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange.

**Community of practice (CoP)**

A community of practice (CoP) is a group of people who regularly interact to collectively learn, solve problems, build skills and competencies, and develop best practices around a shared concern, goal, mission, set of problems, or work practice. CoPs cut across formal organizational structures and increase individual and organizational agility and responsiveness by enabling faster learning, problem solving, and competence building; greater reach to expertise across the force; and quicker development and diffusion of best practices. CoP structures range from informal to formal and may also be referred to as structured professional forums, knowledge networks, or collaborative environments.

**Compatibility**

The capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference.

**Compliance**

A system that meets, or is implementing an approved plan to meet, all applicable Technical Architecture (TA) mandates.

**Component**

One of the subordinate organizations that constitute a joint force. Normally, a joint force is organized with a combination of Service and functional components. An assembly or any combination of parts, subassemblies, and assemblies mounted together in manufacture, assembly, maintenance, or rebuild.

**Concept**

A document or theory that translates a vision or visions into a more-detailed, but still abstract, description of some future activity or end-state, principally concerned with a 3–15 year time frame.

**Configuration**

An expression in functional terms (that is, expected performance) and in physical terms (that is, appearance and composition).

**Connection fee**

The charge, if any, imposed on a subscriber by the cable television (CATV) franchisee for initial hookup, reconnection, or relocation of equipment necessary to transmit the CATV signal from the distribution cable to a subscriber's receiver.

**Context**

The inter-related conditions that compose the setting in which the Architectures exist. It includes environment, doctrine, and tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions.

**Cookie**

A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. They allow user-side customization of Web information. Normally, cookies will expire after a single session.

**Copying**

See *duplicating/copying*.

**Cost-effective**

Describes the course of action that meets the stated requirement in the least costly method. Cost-effectiveness does not imply a cost savings over the existing or baseline situation; rather, it indicates a cost savings over any viable alternative to attain the objective.

**Data**

The representation of facts, concepts, or instructions in a formalized manner which is suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is, or might be, assigned (see JCS 1-02).

**Database**

A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications.

**Data element**

A basic information unit template built on standard semantics and structures that in turn governs the distinct values of one or more columns of data within a row of data within a database table or a field within a file.

**Data management**

The process of creating a basis for posting, sorting, identifying and organizing the vast quantities of data available to DOD.

**Data model**

A graphical and textual representation of data needed by an organization to represent achievement of its mission, functions, goals, objectives, and strategies. A data model is represented by its entities, attributes, and relationships among its entities. In the relational model of data, entities are tables, attributes are columns, and relationships are primary and foreign key pairs. Data models may be enriched beyond data structures with both constraints and embedded processes.

**Data performance plan (DPP)**

An organized and structured approach to the specification and collection of enterprise artifacts in support of community of interest (COI) objectives that operate in a common and shared fashion. Data performance planning collects, develops, and maintains these artifacts and is of primary interest to information system professionals charged with ensuring that information systems meet the needs of the COI. These artifacts are often referred to as "metadata."

**Data Performance Plan System (DPPS)**

A centralized repository for enterprise-wide storing, viewing, and reusing architectures, data models, business rules, and other artifacts associated with functional Army systems.

**Data standards**

Metadata expressed as authoritative data sources (ADSs), information exchange standards specifications (IESSs), enterprise identifiers (EIDs), and eXtensible Markup Language (XML) used to guide all data exchanges including those with legacy systems.

**Data synchronization**

Policies and procedures that govern consistency, accuracy, reliability, and timeliness of data used and generated by the Army. It addresses data planning, storage, scheduling, maintenance, and exchange among authorized users.

**Defense Automated Visual Information System (DAVIS)**

DOD-wide automated catalog system for management of VI products and multimedia material (includes production, procurement, inventory, distribution, production status, and archival control of multimedia/VI productions and materials). The DAVIS will be searched prior to any start of a new VI production to determine if a suitable product already exists. Armed Forces Information Service/DVI is the database manager and provides policy guidance concerning the operation of DAVIS functions. The Web site is <http://dodimagery.afis.osd.mil>.

**Defense Telephone System (DTS)**

A centrally managed system that, in accordance with its charter, provides telephone service to all the DOD activities in the area.

**Degauss**

A procedure that reduces the magnetic flux of a medium to virtually zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable.

**Department of Army Multimedia/Visual Information Production and Distribution Program (DAMVIPDP)**

Provides for the annual identification, funding, and acquisition of multimedia/VI production and distribution requirements. All Army organizations identify their requirements for multimedia/VI productions and forward their requests to their supporting regional/FOA VI manager for validation. Regional/FOA VI managers forward valid requirements to CIO/G-6 for validation.

**Digital signature**

The product of an asymmetric cryptographic system that is created when the owner of the private signing key uses that key to create a unique mark (the signature) on an electronic document or file. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who they claim to be.

**Direct reporting unit (DRU)**

An operational command that reports to and is under the direct supervision of an HQDA element. A DRU executes policy developed by its HQDA principal.

**Disk**

As applied to information management, disc and disk are synonymous. Flat, circular information system media used to record, store, manipulate, and retrieve data and information. Examples of discs are phonograph records, videodisks, computer disks, floppy disks, optical disks, and compact disks.

**Doctrine**

Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative, but requires judgment in application. Doctrine represents consensus on how the Army conducts operations today.

**Domain**

An area of common operational and functional requirements. Currently, there are four domains: command, control, communications, and intelligence (C3I); weapon systems; modeling and simulation; and sustainment.

**Duplicating/copying**

Production of not more than 5,000 units of a single page or not more than 25,000 units in the aggregate of multiple pages produced utilizing automatic copy-processing or copier-duplicating machines employing electrostatic, thermal, or other copying processes.

**Electronic Army (e-Army)**

The strategic employment of IT to provide products, services, or knowledge to intended users—whether they are customers, constituents, internal operations employees, information providers, or business partners—that results in



enhanced value to the user. E-Army encompasses the full range of self-service applications available on AKO, Web services; enterprise resource planning systems; e-content, e-record, and e-pubs programs; e-commerce activities; digital signature; and automated processes that facilitate knowledge exchange.

**Electronic business (e-business)**

A means of performing enterprise activities that involves the use of electronic technologies, including such techniques as facsimile, e-mail, World Wide Web software, electronic bulletin boards, electronic funds transfer, purchase cards, and electronic data interchange.

**Electronic government (e-government)**

The use by government of information technologies that have the ability to transform relations with citizens, employees, businesses partners, and other government organizations. Analogous to e-commerce, which allows businesses to transact with each other more efficiently and brings customers closer to businesses, e-government aims to make the interaction between government and citizens, government and business enterprises, and interagency relationships more friendly, convenient, transparent, and inexpensive.

**Electronic mail (e-mail)**

An information dissemination and retrieval service accessed through distributed user workstations normally provided through office automation initiative.

**Electronic recordkeeping**

The operation of recordkeeping systems requiring a machine interface for the human use of records. Examples of record media include magnetic tapes, disks and drums, video files, and optical disks.

**Electronic signature**

A generic term encompassing both noncryptographic and cryptographic methods of authenticating identity. Noncryptographic methods include PIN or password, smart card, digitized signature, and biometrics. Cryptographic methods include shared symmetric key cryptography, and public/private key (asymmetric) cryptography-digital signatures.

**Enterprise**

The highest level in an organization; it includes all missions, tasks, and activities or functions.

**Enterprise Architecture**

The explicit description of the current and desired relationships among business and management processes and IT. An enterprise architecture describes the “target” situation that the agency wishes to create and maintain by managing its IT portfolio.

**Enterprise identifier (EID)**

A 64-bit information identification tag (key) that remains unique across an enterprise. Each EID is composed of a 32-bit EID seed followed by a 32-bit sequence determined by the EID server.

**Environment**

The conditions (physical, political, economic, and so on) within which an architectural configuration must operate.

**Executive control and essential command supervision (ECECS)**

Those managerial staff functions and positions located above the direct program managerial and operational level of individual morale, welfare, and recreation (MWR) programs that support planning, organizing, directing, coordinating, and controlling the overall operations of MWR programs. ECECS consists of program, fiscal, logistical, and other managerial functions that are required by DODD 1015.2 to ensure oversight. AR 215–1 provides clarification of ECECS with respect to Army MWR programs and activities as those functions and positions that support planning, organizing, directing, coordinating, and controlling the overall operations of MWR programs. ECECS consists of program, fiscal, logistical, and other managerial fiduciary functions that are required to ensure oversight of Government appropriated and nonappropriated fund MWR assets.

**EXtensible Markup Language (XML)**

A tagging language used to describe and annotate data so it can be consumed by human and system interactions. XML is typically arranged hierarchically using XML elements and attributes. It also uses semantically rich labels to describe elements and attributes to enable meaningful comprehension.

**Extranet**

Similar to an Intranet, an extranet includes outside vendors and uses Web technology to facilitate interbusiness transactions, such as placing and checking orders, tracking merchandise, and making payments.

**Facsimile**

A system of telecommunications for the transmission of fixed images with a view to their reception in a permanent form. These images include typewritten and handwritten documents, fingerprint records, maps, charts, operations overlays, sketches, and low resolution photographs.

**Franchise**

Authorization, or renewal thereof, issued by a franchising authority, whether such authorization is designated as a franchisee, permit, license, resolution, contract, certificate, agreement, or otherwise, which authorizes the construction or operation of a cable system.

**Franchisee**

Any individual or partnership, association, joint stock company, trust corporation who owns or controls, is owned or controlled by, or is under common ownership or control with such person.

**Function**

Within the context of the AEA framework, a synonym for activity.

**Functional proponent**

Commander or chief of an organization or staff element that is the operative agency charged with the accomplishment of a particular function(s) (see AR 5–22).

**Government Performance and Results Act (P.L. 103–62)**

A law that creates a long-term goal-setting process to improve Federal program effectiveness and public accountability by promoting a new focus on results, service quality, and customer satisfaction.

**Graphic arts**

Relates to the design, creation, and preparation of two- or three-dimensional visual products. Includes charts, graphics, posters, and visual materials for brochures, covers, television, motion pictures, printed publications, display, presentations, and exhibits prepared manually, by machine, or by computer.

**Hardware**

The generic term dealing with physical items as distinguished from the capability or function, such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object. In data automation, the physical equipment or devices forming a computer and peripheral components. (See also software.)

**Imagery**

A pictorial representation of a person, place, thing, idea, or concept, either real or abstract, used to convey information.

**Information**

The meaning that a human assigns to data by means of the known conventions used in their representations (see JCS 1–02). Information is a shared resource and is not owned by any organization within the restrictions of security, sensitivity, and proprietary rights.

**Information Assurance Vulnerability Alerts (IAVA)**

Positive control mechanism that pushes alerts and advisories on IA security vulnerabilities to IA personnel. IAVA also requires the tracking of response and compliance to the messages.

**Information exchange requirement**

Substantive content, format, throughput requirements, and classification level.

**Information exchange standards specification (IESS)**

A narrowly scoped data model to facilitate data exchange and interoperability between communities of interest.

**Information management**

Planning, budgeting, manipulating, and controlling of information throughout its life cycle.

**Information requirement**

The expression of need for data or information to carry out specified and authorized functions or management purposes that require the establishment or maintenance of forms or formats, or reporting or recordkeeping systems, whether manual or automated.

**Information resources management (IRM)**

The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, maintenance, utilization, dissemination, and disposition of information, regardless of media; includes the management of information and information-related resources and systems, whether manual or automated, such as records management activities, privacy and security of records, agency sharing and dissemination of information, and acquisition and use of automatic data processing, telecommunications, and other IT.

**Information system**

The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. For the purposes of AITR, the terms “application” and “information system” are used synonymously—a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. The application of IT to solve a business or operational (tactical) problem creates an information system.

**Information Technology (IT)**

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment, or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “information technology” also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term “information technology” does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (Ref. Clinger–Cohen Act of 1996.)

**Infostructure**

The shared computers, ancillary equipment, software, firmware and similar procedures, services, people, business processes, facilities (to include building infrastructure elements) and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of data or information in any format including audio, video, imagery, or data, whether supporting Information Technology or National Security Systems as defined in the Clinger–Cohen Act of 1996.

**Infrastructure**

The term is used with different contextual meanings. It most generally relates to and has a hardware orientation, but it is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs.

**Installation**

Geographic area subject to the control of the installation commander, including Government-owned housing or supported activities outside the perimeter of the military installation which depend on it for support.

**Integration**

The process of making or completing by adding or fitting together into an agreed framework (architecture) the information requirements, data, applications, hardware, and systems software required to support the Army in peace, transition, and conflict.

**Integrity (of information)**

Assurance of protection from unauthorized change.

**Internet**

An electronic communications network that connects computer networks and organizational computer facilities around the world.

**Internet Service Provider (ISP)**

A organization that provides other organizations or individuals with access to, or presence on, the Internet. Most ISPs also provide extra services including help with design, creation and administration of World Wide Web sites, training, and administration of intranets.

**Interface**

A boundary or point common to two or more similar or dissimilar telecommunications systems, subsystems, or other entities at which necessary information flows take place.

**Interoperability**

The ability of two or more systems, units, forces, or physical components to exchange and use information. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily.

**Intra-Army interoperability certification**

Confirmation from CIO/G-6, based on the recommendation of the Central Technical Support Facility (CTSF) Director, that the candidate system has undergone appropriate testing and that the applicable standards and requirements for compatibility, interoperability, and integration have been met.

**Intranet**

A computer network that functions like the Internet, using Web browser software to access and process the information that employees need, and located on computers within the organization/enterprise. A firewall is usually used to block access from outside the intranet. Intranets are private Web sites.

A private Internet operating on an organization's internal network; an information utility that makes organizational and departmental information accessible via the standards of the Internet: e-mail (SMTP), WWW, file transfer protocol, and other Internet services.

**IT Architecture**

An integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the agency's strategic and information resources management goals.

**IT capital planning and investment control**

An end-to-end integrative process that frames and manages the life cycle of an IT investment. Its purpose is to maximize the value and assess and manage the risks of the IT acquisitions of the Army. The process includes the selection, management, and evaluation of IT investments.

**IT investment portfolio**

A collection of IT investments that represents the best balance of costs, benefits, and risks and is designed to improve the overall organizational performance and maximize mission performance.

**IT management process**

An end-to-end integrated process that includes the information management/information technology (IM/IT) business planning, business/functional process improvement, capital investment planning and investment control IT management and oversight, acquisition of C4/IT, fielding and prioritization.

**IT support agreement**

An agreement to provide recurring IT support, the basis for reimbursement (if any) for each category of support, the billing and payment process, and other terms and conditions of the agreement.

**Joint Technical Architecture-Army (JTA-A)**

The complete set of rules derived from the JTA that prescribe the technical standards for Army IT systems and enable interoperability among joint systems.

**Life cycle**

The total phases through which an item progresses from the time it is initially developed until the time it is either consumed, in use, or disposed of as being excess.

**Machine readable**

Data and information storage media requiring the use of one or more information system component(s) for translation into a medium understandable and usable to humans.

**Management Decision Evaluation Package (MDEP)**

An 8-year package of dollars and manpower to support a given program or function. The BIP is the first 3 budget and execution years of the MDEP, and the PDIP is the 5 program years following.

**Master/community antenna television (M/CATV) system**

A facility consisting of a television reception service that receives broadcast radio frequency television signal and/or FM radio programs and distributes them via signal generation, reception, and control equipment.

**Master plan**

An enterprise-wide planning directive that establishes the vision, goals, and objectives of the enterprise; establishes an enterprise-level procedure for achieving the vision, goals, and objectives; specifies actions required to achieve the vision, goals, and objectives; identifies roles and assigns responsibilities for executing the specified actions; establishes priorities among actions and relevant supporting programs; and establishes performance measures and responsibilities for measuring performance.

**Measure**

One of several measurable values that contribute to the understanding and quantification of a key performance indicator.

**Message (telecommunications)**

Record information expressed in plain or encrypted language and prepared in a format specified for intended transmission by a telecommunications system.

**Metadata**

Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings.

**Metrics**

The elements of a measurement system consisting of key performance indicators, measures, and measurement methodologies.

**Mission**

A group of tasks, with their purpose, assigned to military organizations, units, or individuals for execution.

**Mission critical (MC) information system**

A system that meets the definitions of "information system" and "national security system" in the Clinger–Cohen Act, the loss of which would cause the stoppage of war fighter operations or direct mission support of war fighter operations.

**Mission Essential (ME) Information System**

A system that meets the definitions of "information system" and "national security system" in the Clinger–Cohen Act, that the acquiring component head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The definition of "the Organizational Mission" is one of the organizational missions of the Army—not just a single MACOM or DA functional proponent.)

**Mission-related**

Processes and functions that are closely related to the mission (for example, the mission of Direct and Resource the Force has the mission-related functions of planning, programming, policy development, and allocating of resources).

**Morale, welfare, and recreation (MWR) programs**

Military MWR programs (exclusive of private organizations as defined in DODI 1000.15) located on DOD installations

or on property controlled (by lease or other means) by DOD or furnished by a DOD contractor that provide for the mission sustainment and community support for authorized DOD personnel.

**Motion media**

A series of images viewed in rapid succession, giving the illusion of motion, obtained with a motion picture or video camera.

**Multimedia**

The synchronized use of two or more types of media, regardless of the delivery medium.

**National Security System**

Any telecommunications or information system operated by the United States Government, the function, operation, or use of which 1) involves intelligence activities, 2) involves cryptologic activities related to national security, 3) involves command and control of military forces, 4) involves equipment that is an integral part of a weapon or weapons system, or 5) is critical to the direct fulfillment of military or intelligence missions (ref. the Clinger–Cohen Act of 1996).

**Negotiation**

The communication by any means of a position or an offer on behalf of the United States, DOD, or any office or organizational element thereof, to an agent or representative of a foreign government (including an agency, instrumentality, or political subdivision thereof) or of an international organization in such detail that the acceptance in substance of such position or offer would result in an international agreement. The term also includes any communication conditional on subsequent approval by higher authority but excludes mere preliminary, exploratory, or informal discussions or routine meetings conducted on the understanding that the views communicated do not and will not bind any side. (Normally, the approval authority will authorize the requesting command to initiate and conduct the negotiation.)

**Networthiness**

Risk management accomplished through the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the Army enterprise.

**News clip**

A news story of an event recorded and released on motion picture or videotape for viewing by an internal Army audience or the general public.

**Nonappropriated fund(s) (NAF)**

Cash and other assets received from sources other than monies appropriated by the Congress of the United States. (NAF must be resources of an approved NAFL.) NAF are U.S. Government funds, but they are separate and apart from funds that are recorded in the books of the Treasury of the United States. They are used for the collective benefit of the authorized patrons who generate them.

**Nonappropriated fund instrumentalities (NAFIs)**

Every NAFI is legally constituted as an “instrumentality of the United States.” Funds in NAFI accounts are Government funds, and NAF property, including buildings, is Government property. However, NAF are separate from appropriated funds (APF) of the U.S. Treasury. They are not commingled with APF and are managed separately, even when supporting a common program or activity.

**Nonpublic data/information**

Data/information that is personally identifiable and subject to the Privacy Act, classified according to the National Security Act, subject to a Freedom of Information Act exemption, or sensitive.

**Objectives**

Quantified goals identifying performance measures that strive to improve the effectiveness or efficiency of agency programs in support of mission goals.

**Operational Architecture**

Descriptions of the tasks, operational elements, and information flows required to accomplish or support a function.

**Operational View (OV) (Architecture)**

A description (often graphic) of the operational elements, assigned tasks, and information flows required to accomplish

or support a warfighting function. It defines the type of information, the frequency of exchange, and the tasks supported by these information exchanges.

**Operational requirement**

A formally established, validated, and justified need for the allocation of resources to achieve a capability to accomplish approved military objectives, missions, or tasks.

**Organizational messaging**

Correspondence that is used to conduct the official business of the Army. Any message that commits resources, directs action, clarifies official position or issues official guidance is considered an organizational message.

**Performance management**

The use of performance measurement information to help set agreed-upon performance goals, allocate and prioritize resources, inform managers to either confirm or change current policy or program directions to meet those goals, and report on the success in meeting those goals.

**Performance measure**

A quantitative or qualitative characterization of performance.

**Performance measurement**

A process of accessing progress toward achieving predetermined goals, including information on the efficiency with which resources are transformed into goods and services (outputs), the quality of those outputs (how well they are delivered to clients and the extent they are satisfied), and outcomes (the results of a program activity compared to its specific contributions to program objectives).

**Periodical**

A nondirective classified or unclassified Army magazine or newsletter-type publication published annually or more often to disseminate information necessary to the issuing activity with a continuing policy regarding format, content, and purpose. A periodical is usually published to inform, motivate, increase knowledge, or improve performance. It contains official or unofficial information or both.

**Permanent record**

Information that has been determined by the Archivist of the United States to have sufficient value to warrant its preservation by the National Archives and Records Administration for the life of the Republic.

**Persistent cookies**

Cookies that can be used to track users over time and across different Web sites to collect personal information.

**Photojournalism**

Conveying a story, through still photography, of a significant DOD event, normally to support the news media or internal DOD publications.

**Planning, Programming, Budgeting, and Execution (PPBE) process**

The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

**Printing**

The processes of composition, platemaking, presswork, and binding, including micropublishing, for the production of publications.

**Process**

A group of logically related decisions and activities required to manage the resources of the Army. A business process is a specific ordering of work activities across time and place, with a beginning, an end, and clearly defined inputs and outputs that deliver value to customers.

**Process owners**

HQDA functional proponents, MACOMs, and others who have responsibility for any mission-related or administrative work process.

**Procurement/contracting**

Purchasing, renting, leasing, or otherwise obtaining supplies or services from non-Federal sources. Includes description

(but not determination) of supplies and services required, selection and solicitation of sources, preparation and award of contracts, and all phases of contract administration. Does not include making grants or cooperative agreements.

**Proponent**

An Army organization or staff that has been assigned primary responsibility for material or subject matter in its area of interest.

**Publications**

Items of information that are printed or reproduced, whether mechanically or electronically, for distribution or dissemination usually to a predetermined audience. Generally, they are directives, books, pamphlets, posters, forms, manuals, brochures, magazines, and newspapers produced in any media by or for the Army.

**Publicly accessible Web site (or public Web site) on the World Wide Web**

Army Web site with access unrestricted by password or PKI user authorization. "Public" refers to the at-large audience on the Internet; anyone who can access a Web site through a browser.

**Publishing**

Actions involved in issuing publications; involves creating, preparing, coordinating, approving, processing, printing, and distributing or disseminating publications.

**Record**

All books, papers, maps, photographs, machine readable items (such as, disks, tapes, cards, printouts, aperture cards, roll microfilm, microfiche, laser disk, optical disk, optical card, other optical recording media, film slides, transparencies, or other documentary materials regardless of physical form or characteristics) made or received by any entity of the Department of the Army as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities because of the informational value of the data.

**Records centers**

Locations established in CONUS to receive and maintain records with long-term or permanent value, pending their ultimate destruction or accession into the National Archives.

- a. Federal records centers: records centers operated by the National Archives and Records Administration.
- b. Army records centers: Army-maintained records centers for intelligence, criminal investigation, and similar records.

**Records management**

The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with information creation, information maintenance and use, and information disposition in order to achieve adequate and proper documentation of the policies, transactions, and effective and economical management of DA operations.

**Records management program**

A program that includes elements concerned with the life-cycle management of information, regardless of media. Specific elements include the management of correspondence, reports, forms, directives and publications, mail, distribution, maintenance (use and disposition of recorded information), declassification of recorded information, and the implementation of responsibilities under the Freedom of Information Act and the Privacy Act.

**Requirements generation process**

The formal method of determining military operational deficiencies and the preferred set of solutions.

**Satellite communications (SATCOM)**

DOD use of military-owned and operated satellite communication space systems that use Government frequency bands, and commercial satellite communication systems provided by commercial entities using commercial frequency bands. SATCOM is further defined to include DOD's use of other allied and civilian satellite communications resources as appropriate (See CJCSI 6250.01). SATCOM includes Defense Satellite Communications System (DSCS), DOD Teleport integration of C, Ku, Ka, UHF, EHF, advanced EHF and Mobile User Objective System (MUOS), MILSTAR, Teleport, Wideband Gapfiller System (WGS), and Defense Information Infrastructure.

**Service level agreement (SLA)**

A formal agreement between the customer(s) and the service provider specifying service levels and the terms under which a service or a package of services is provided to the customer.



**Sensitive compartmented information (SCI)**

Information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term encompasses COMINT and Special Activities Office information and materials.

**Smart card**

A credit card-size device, normally for carry and use by personnel, that contains one or more integrated circuit chips and may also employ one or more of the following technologies: 1) magnetic stripe; 2) barcodes, linear or two dimensional; 3) noncontact, radio frequency transmitters; 4) biometric information; 5) encryption and authentication; and 6) photo identification. It may be used to generate, store, or process data.

**Software**

A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system (for example, compiler, library routines, manuals, circuit diagrams); usually contrasted with hardware.

**Spam**

Widely disseminated “junk” mail.

**Standard**

Within the context of the Army Enterprise Architecture, a document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. It may also establish requirements for selection, application, and design criteria of materiel.

**Still photography**

The medium used to record still imagery; includes negative and positive images.

**Strategic planning**

A continuous and systematic process whereby guiding members of an organization make decisions about its future, develop the necessary procedures and operations to achieve that future, and determine how success is to be measured.

**Subscriber**

Any person, group, organization (including concessionaire), or appropriated or nonappropriated fund activity that procures services made available pursuant to the terms of the franchise agreement.

**Support agreement**

An agreement to provide recurring BASOPS support to another DOD or non-DOD federal activity.

**Synchronization**

Coordinating and aligning the development of the Army Enterprise Architectures in both timing and direction for mutual reinforcement and support.

**System**

An organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions (see JCS 1–02). Within the context of the Army Enterprise Architecture, systems are people, machines and methods organized to accomplish a set of specific functions; provide a capability or satisfy a stated need or objective; or produce, use, transform, or exchange information. For the purpose of reporting to the Army Information Technology Registry, the terms “application” and “system” are used synonymously—a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information (that is, the application of IT).

**Synchronization**

See data synchronization.

**Systems Architect**

Responsible for integration and oversight of all Army information systems.

**Systems Architecture**

Descriptions, including graphics, of systems and interconnections providing for or supporting functions

**System View (SV) (Architecture)**

A description, including graphics, of systems and interconnections, providing for or supporting warfighting functions. It defines the physical connection, location, and identification of key nodes, circuits, networks, and warfighting platforms and specifies system and component performance parameters. It shows how multiple systems within a subject area link and interoperate and may describe the internal construction or operations of particular systems.

**The Army Plan**

This plan is a 16-year strategic planning horizon that includes the 6-year span of the program (POM) years plus an additional 10 years. TAP presents comprehensive and cohesive strategic, midterm planning and programming guidance that addresses the Army's enduring core competencies over this time period.

**Task**

A discrete event or action, not specific to a single unit, weapon system, or individual, that enables a mission or function to be accomplished by individuals or organizations.

**Technical Architecture (TA)**

The technical architecture provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed.

**Technical control (TECHCON)**

The authority for one organization or command to issue and enforce policy and authoritative direction concerning the use of techniques, procedures, standards, configurations, designs, devices, and systems to another specified organization to accomplish a specific mission. It does not include command authority or administrative control for logistics or matters of administration, discipline, internal organization, or unit training. NETCOM will exercise TECHCON over all organizations that operate and maintain portions of the AEI.

**Technical View (TV) (Architecture)**

The minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements of a system to ensure that a system satisfies a specified set of requirements. A TV identifies services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed.

**Telecommunications**

Any transmission, emission, or reception of signs, signals, writings, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems.

**Telework**

Working at an alternative site via use of electronic means.

**TEMPEST**

An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security.

**Third-party cookies**

Cookies placed on a user's hard drive by Internet advertising networks. The most common third-party cookies are placed by the various companies that serve the banner ads that appear across many Web sites.

**User**

Any person, organization, or unit that uses the services of an information processing system. Specifically, it is any table of organization and equipment (TOE) or table of distribution and allowances (TDA) command, unit, element, agency, crew or person (soldier or civilian) operating, maintaining, and/or otherwise applying DOTMLPF products in accomplishment of a designated mission.

**URL (uniform resource locator)**

A Web address a person uses to direct a browser program to a particular Internet resource (for example, a file, a Web page, an application, and so on). All Web addresses have a URL.

**User fee**

The periodic service charge paid by a subscriber to the franchisee for service.

**Video**

Pertaining to bandwidth and spectrum position of the signal that results from television scanning and is used to produce an electronic image.

**Video teleconferencing**

Two-way electronic voice and video communication between two or more locations; may be fully interactive voice or two-way voice and one-way video; includes full-motion video, compressed video and sometimes freeze (still) frame video.

**Vision**

A description of the future; the most abstract description of the desired end-state of an organization or activity at an unspecified point in the future.

**Visual information (VI)**

Information in the form of visual or pictorial representations of person(s), place(s), or thing(s), either with or without sound. VI includes still photographs, digital still images, motion pictures, analog and digital video recordings, and hand- or computer-generated art and animations that depict real or imaginary person(s), place(s), and/or thing(s), and related captions, overlays, and intellectual control data.

**VI activity**

An organizational element or a function within an organization in which one or more individuals are classified as visual information (VI) specialists, or whose principal responsibility is to provide VI services. VI activities include those that expose and process original photography; record, distribute, and broadcast electronically (video and audio); reproduce or acquire VI products; provide VI services; distribute or preserve VI products; prepare graphic artwork; fabricate VI aids, models, and displays; and provide presentation services or manage any of these activities.

**VI documentation (VIDOC)**

Motion media, still photography, and audio recording of technical and nontechnical events, as they occur, and are usually not controlled by the recording crew. VIDOC encompasses combat documentation (COMDOC), operational documentation (OPDOC), and technical documentation (TECDOC).

**VI equipment**

Items capable of continuing or repetitive use by an individual or organization for the recording, producing, reproducing, processing, broadcasting, editing, distribution, exhibiting, and storing of visual information. Items otherwise identified as VI equipment that are an integral part of a non-VI system or device (existing or under development), will be managed as a part of that non-VI system or device.

**VI functions**

The individual VI processes, such as production, documentation, reproduction, distribution, records preservation, presentation services, VI aids, fabrication of model and displays, and related technical services.

**VI library**

A VI activity that loans, issues, and maintains an inventory of motion media, imagery and/or equipment.

**VI management office**

Staff office at a NETCOM/9th ASC region, FOA, or other management level established to prescribe and require compliance with policies and procedures, and to review operations.

**VI materials**

A general term, which refers collectively to all of the various VI still and motion films, tapes, discs, or graphic arts. Includes the original, intermediate and master copies, and any other retained recorded imagery.

**VI production**

The combination of motion media with sound in a self-contained, complete presentation, developed according to a plan or script for purpose of conveying information to, or communicating with, an audience. A production is also the end item of the production process. Used collectively, VI production refers to the functions of procurement, production or adoption from all sources, such as in-house or contract production, off-the-shelf purchase, or adoption from another Federal agency.

**VI products**

VI media elements such as motion picture and still photography (photographs, transparencies, slides, film strips), audio and video recordings (tape or disc), graphic arts (including computer-generated products), models, and exhibits.

**VI records**

VI materials, regardless of format, related captions, and intellectual control data.

**VI records center**

A facility, sometimes specially designed and constructed, for the low-cost and efficient storage and referencing of semicurrent records pending their ultimate disposition.

**VI report**

VI documentation assembled to report on a particular subject or event.

**VI resources**

The personnel, facilities, equipment, products, budgets, and supplies which comprise DOD visual information support.

**VI services**

Those actions that 1) result in obtaining a visual information product; 2) support the preparation of a completed VI production such as photographing, processing, duplicating, sound and video recording, instrumentation recording, and film to video transferring, editing, scripting, designing, and preparing graphic arts; 3) support existing VI products such as distribution and records center operations; and 4) use existing VI products, equipment, maintenance, and activities to support other functions such as projection services, operation of conference facilities, or other presentation systems.

**VI Support Center (VISC)**

The VI activity that provides general support to all installation, base, facility or site organizations or activities. It may include motion picture, still photo, television, and audio recording for nonproduction documentary purposes, their laboratory support, graphic arts, VI libraries, and presentation services.

**Warfighter**

A common soldier, sailor, airman, or marine by trade, from all Services who joins in a coordinated operation to meet a common enemy, a common challenge, or a common goal.

**Warfighting requirements**

Requirements for ACAT I–IV systems or IT capabilities in direct use by or support of the Army warfighter in training for and conducting operational missions (tactical or other), or connecting the warfighter to the sustaining base.

**Web portals**

Web sites that serve as starting points to other destinations or activities on the Web. Initially thought of as a “home base” type of Web page, portals attempt to provide all of a user’s Internet needs in one location. Portals commonly provide services such as e-mail, collaboration centers, online chat forums, searching, content, newsfeeds, and others.

**Web site**

A location on the Internet; specifically it refers to the point of presence location in which it resides. All Web sites are referenced using a special addressing scheme called a URL. A Web site can mean a single HTML file or hundreds of files placed on the net by an enterprise.

**World Wide Web (WWW)**

A part of the Internet designed to allow easier navigation of the network through the use of graphical user interfaces and hypertext links between different addresses—called also “Web.”

**Section III****Special Abbreviations and Terms**

This section contains no entries.

**UNCLASSIFIED**

**PIN 058039-000**

# USAPD

ELECTRONIC PUBLISHING SYSTEM  
OneCol FORMATTER WIN32 Version 216

PIN: 058039-000

DATE: 06-25-04

TIME: 09:27:51

PAGES SET: 125

---

DATA FILE: C:\wincomp\r25-1.fil

DOCUMENT: AR 25-1

SECURITY: UNCLASSIFIED

DOC STATUS: REVISION